2007-06

Performance of wireless unattended sensor networks in maritime applications

Casias, Juan Francisco.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/3497

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PERFORMANCE OF WIRELESS UNATTENDED SENSOR NETWORK IN MARITIME APPLICATIONS

by

Juan Francisco Casias

June 2007

Thesis Advisor: John C. McEachen
Second Reader: Weilian Su

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Performance of Wireless Unattended Sensor Network in Maritime Applications			**5. FUNDING NUMBERS**
6. AUTHOR(S) Juan Francisco Casias			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Wireless, unattended sensor networks offer a superior monitoring capability with unparalleled flexibility. Traditional systems are typically restrictive in the rigidity of their positioning and topological design requirements. Ongoing research continues to expand the potential for the use of these un-tethered and autonomous systems ranging from the mundane, monitoring soil conditions for agricultural crops, to the extreme of military operations, providing valuable intelligence to commanders in a variety of battle-space conditions.

This thesis investigated the use of this type of system in what may be the most hostile of environmental conditions from a wireless networking and communications point of view, the water. The network will be required to organize, establish and maintain itself in a variety of dynamic conditions in or on the water. Commercial off-the-shelf products developed by Crossbow Technologies were used in developing the wireless, unattended sensor network consisting of single and multiple nodes. Nodes were tested on a solid ground surface, on the surface of the water, below the surface of the water (not submerged), and fully submerged. The most significant findings were attained with regard to range. Other findings with regard to link quality, network formation, and network stability support results attained in previous research.

14. SUBJECT TERMS Wireless Sensor Network, TinyOS, XMesh Routing Protocol, Network Stability, Link Connectivity.			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PERFORMANCE OF WIRELESS UNATTENDED SENSOR NETWORKS IN MARITIME APPLICATIONS

Juan Francisco Casias
Lieutenant, United States Navy
B.S., University of Idaho, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2007

Author: Juan Francisco Casias

Approved by: John C. McEachen
Thesis Advisor

Weilian Su
Second Reader

Jeffrey B. Knorr
Chairman, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Wireless, unattended sensor networks offer a superior monitoring capability with unparalleled flexibility. Traditional systems are typically restrictive in the rigidity of their positioning and topological design requirements. Ongoing research continues to expand the potential for the use of these un-tethered and autonomous systems ranging from the mundane, monitoring soil conditions for agricultural crops, to the extreme of military operations, providing valuable intelligence to commanders in a variety of battle-space conditions.

This thesis investigated the use of this type of system in what may be the most hostile of environmental conditions from a wireless networking and communications point of view, the water. The network will be required to organize, establish and maintain itself in a variety of dynamic conditions in or on the water. Commercial off-the-shelf products developed by Crossbow Technologies were used in developing the wireless, unattended sensor network consisting of single and multiple nodes. Nodes were tested on a solid ground surface, on the surface of the water, below the surface of the water (not submerged), and fully submerged. The most significant findings were attained with regard to range. Other findings with regard to link quality, network formation, and network stability support results attained in previous research.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Professor John McEachen for his guidance and support in the research and writing of what has been the greatest technical and literary undertaking of my life.

Also the entire Electrical Engineering Department for their patience and perseverance in my instruction, despite my efforts to resist the impression of progressively higher levels of technical knowledge on my limited intellect.

A special thanks to Jeff Knight, a lab assistant without whom I may never have made it this far.

To CAPT Dave Duryea, without whom my lateral transfer would not have been possible.

To CAPT Howard Trost, without whom my lateral transfer would not have been successful.

Finally, to my wife Jennifer and my daughters Breanna and Sarah, you are the reason I am able to do what I do. Jen, you keep me in line. Girls, you give me hope for the future.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

As technology continues to evolve at an unprecedented rate, more and more technologies become available for use in ways that were heretofore unimagined. Wireless, unattended sensor networks are achieving levels of capability which make them practical for use in a multitude of military applications. Integrated circuits have become smaller, lighter, and less expensive without sacrificing either their reliability or their functionality. This in turn has lead to significant increases in wireless communications and data networking performance thresholds. All of which culminates in a system with the potential to meet military requirements for a plethora of uses.

Wireless, unattended sensor networks consist of nodes capable of performing computations, sensing a variety of parameters, and communicating all of this information wirelessly. The nodes are deployed over the desired area and communicate with a base station (BS) either directly or by proxy via other nodes in the network. The unattended nature of the network rests in its ability to self-organize and maintain itself. The software employed allows the network to adapt to the dynamics of its environment, such as node failures, signal degradations, or changes in node positions. Although many of the risks associated with this type of technology have been dealt with, the potential for problems still exists. Continued research to mitigate the factors that contribute to these is required for development of employment strategies for any military applications.

This thesis investigated the ability of this type of system to perform in a maritime environment. Specifically, performance evaluations were conducted with the nodes on or in the water. Evaluations were conducted with the BS and all nodes resting on the surface of the water and below the surface of the water not fully submerged and fully submerged. Node and network performance were evaluated with respect to network establishment and organization and node communication range and continuity.

A commercial off-the-shelf system developed by Crossbow Technologies was used for the BS and nodes of the network tested. In relation to this, the general characteristics of wireless, unattended sensor networks, the Tiny Micro-Threading

Operating System (TinyOS), and the XMesh routing protocol were discussed. Nodes were tested on a solid ground surface, on the surface of the water, below the surface of the water (not submerged), and fully submerged. The most significant findings were attained with regard to range. Other findings with regard to link quality, network formation, and network stability support results attained in previous research.

I. INTRODUCTION

A. MOTIVATION

Throughout history technological superiority has been at the forefront of military dominance. Wireless, unattended sensor networks stand at the cusp of current technology and are ready for implementation in any field that that can find a use for them. Current military doctrine has come to recognize the need for such a technology. Sea Power 21 [1] affirms the need for long term autonomous sensor systems for the purposes of continuous reconnaissance, surveillance, and intelligence gathering. Joint Power 2020 [2] acknowledges that these systems can augment a force's effectiveness in monitoring and maneuvering a battle-space for more precise, favorable engagements. All of this culminated with the development of an Expeditionary Sensor Grid [3] concept. The grid would include on the order of hundreds, or even thousands, of networked sensor nodes with low power requirements to provide near continuous real time sensor coverage for a period of months, possibly years. Sensors of various types within the grid would be flexibly integrable to seamlessly fuse all data collected.

As technology continues to progress at a prodigious rate the size, weight, and cost of the components necessary to realize these mandates become viable. The maturation of technologies involving integrated circuitry, wireless communications, and data networking make the systems more autonomous without sacrificing processing capability. All of this combines to provide a practical mechanism for the implementation of this type of system. Many of the risks associated with this type of technology have been alleviated, however military applications continue to present additional challenges that must be addressed. [4] Much of the previous work in the field has been accomplished for dry environments. Coming from a background of seagoing vessels, the focus of this work is with relation to watery environments.

B. THESIS OBJECTIVE

The objective of this thesis is to evaluate the performance of wireless, unattended sensor networks in a watery environment. Performance metrics of interest are network formation and organization and communication range and efficiency. These will be assessed with respect to a variety of orientations on and in the water.

The wireless, unattended sensor network used is produced by Crossbow Technologies. This network operates on the TinyOS operating system with the XMesh routing protocol. Between two and eight sensor nodes were used to form the architecture of the network with the BS. Node communication ranges were measured for a variety of conditions. Network formation times, topological changes, and routing efficiencies were also noted under the same conditions.

C. PRIOR WORK

A study by Mark E. Tingle in March 2005 tested the communication and sensor ranges of the MICA2 mote at a fixed radio transmission power over four types of terrain. The four terrain types were open terrain, outdoor wooded terrain, urban outdoor terrain and indoor terrain. The tests were conducted at ground level and two heights, six and twelve inches off the ground. The study found that the radio ranges varied between five to nineteen meters. It was noted that communication at ground level was never greater than six meters and the longest connectivity recorded was nineteen meters with the mote at twelve inches off the ground in the indoor environment. The study also tested the characteristics of the different types of sensors that can be used in wireless sensor networks and the viability of their use in military applications. This information is of particular interest in comparison to similar data obtained in the experimentation performed for this thesis. [5]

A study by Cheng Kiat Amos, Teo in December 2005 tested the connectivity ranges of motes using the XMesh routing protocol for multiple power settings. XMesh

proved adaptable, reliable, and stable under a variety of stressors at all power levels. The study also performed an energy efficiency study to explore various means of extending network longevity. [6]

A study by Swee Jin Koh in March 2006 provides a detailed study of the performance of mote antennas and their radiation characteristics. [7]

A new approach for electromagnetic (EM) wave propagation through seawater was presented in a paper in November, 2004. Experiments were conducted in a laboratory as well as real seawater environments. [8]

In 2003, a small underwater robot was designed for experiments with sensor-actuator networks. The MICA2 mote platform, which is used extensively in the sensor networking community as an experimental testbed, was the basis for the robot. Depth regulation and temperature measurement were reported and analyzed in preliminary tests. [9]

D. THESIS ORGANIZATION

This chapter has presented the motivation for and the objectives for this thesis. The following chapters are organized in the following manner. Chapter II will present a general introduction to and overview of wireless sensor networks. This will include a discussion of network architectures and protocols, some challenges associated with networks, as well as some current applications of these networks. Chapter III will delve into more detail about the network actually being implemented for this study. This will include some specifics about the operating system and routing protocol and some prior work using the same system. Chapter IV will cover the experimental study conducted for this thesis. Finally, Chapter V will go over the conclusions of this thesis and some recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS SENSOR NETWORKS

A. CHAPTER OVERVIEW

This chapter introduces the general concepts related to wireless sensor networks and their constituent components. The architectures and protocols involved with these types of networks will then be discussed. This will be followed by a discussion of some of the challenges and applications also associated with them.

B. INTRODUCTION TO WIRELESS, UNATTENDED SENSOR NETWORKS

Wireless, unattended sensor networks represent an area of research that draws upon a range of different disciplines. Contributions come from, but are not limited to, the studies of communications, networking, information management, distributed algorithms, and embedded systems and architecture. These complex systems meet the requirements to be used in a wide variety of commercial and military applications. Most implementations of these networks demand long stay times while precluding access to the sensor nodes on a regular basis, if at all. Given that the overall network must organize and maintain itself, key design considerations for any such system are sensor node size and power consumption. [10, 11]

1. Characteristics of Wireless, Unattended Sensor Networks

Wireless, unattended sensor networks consist of a scaleable number of distributable, lightweight wireless devices called nodes. Each node possesses sensing, computing, and communication capability. The nodes organize themselves into a network, with one of the nodes designated as the BS. All information is communicated to the BS from a node directly or by being relayed through other nodes in the network. This allows the network to maintain its own viability in a dynamic environment. In this way the nodes can route the information by the most efficient means possible to compensate for failures or changes in their surroundings. The distinguishing characteristics for the

nodes can be summarized as compact, power efficient and self-organizing with a diversity of design and purpose. The highly distributed nature of a wireless, unattended sensor network drives the need for these characteristics. [12]

Efficiency of size and weight are obvious concerns. As integrated circuitry technology improves these become as much issues of power as capability. Integrated circuits seem to diminish in size while growing in capability. Effective system design demand sources of power comparable in size, while maintaining adequate capacity. [12]

Nodes must be able to operate in low power modes to increase the longevity of their power supplies. This aspect of performance can be the most critical. Sensor network stay times on the order of years could be desired and nodes may be deployed in areas where access is nearly impossible. This could be achieved directly by improving battery technology. Though a vast amount of study has been done in this area, progress is slow. A less direct method of achieving the same effect would be to optimize the operation of the network. An example of this would be for the nodes to engage in a sleep mode. In this mode of operation the nodes would only be active for short intermittent periods of time. These periods of time could be at regular intervals or when actively sensing changes in the environment. In either case the size of the battery becomes a limiting factor in the size of the node. [12, 13]

The unattended nature of the network stems from its ability to organize and maintain itself. Each node must be relied upon to perform its integral functions concurrently. These functions are to gather data and to report it. Performing these concurrently strains the network as nodes with limited storage capacity may be called upon to simultaneously capture sensor data as well as relay data from other nodes. Once in place, the nodes will automatically establish the most efficient routing paths and periodically adjust them to provide continuity of information flow for changes in status or surrounding. This is programmed into the software and lends itself directly to ease of scalability and installation and increased reliability. [13 - 15]

a. Sensor Node Components

Sensor nodes can be broken down into five main components. These consist of the processor, memory, sensor, communication device, and the power supply. The processor and memory work together and coordinate the functions of the node. A variety of sensors can be employed based on network employment. The communication device allows the nodes to work together without a physical connection. The power supplies the energy required by the node to carry out its functions. Figure 1 below depicts a basic diagram of sensor node components. [10]

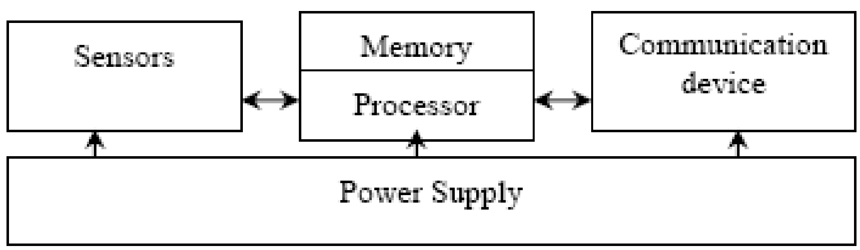

Figure 1. Sensor Node Components

(1) Processor and Memory. At the heart of the node are the processor and its associated memory. The processor executes a variety of programs to collect data from its sensor and process signals from other nodes. It utilizes a series of communications protocols to make decisions on where and when to send its information. Random Access Memory (RAM), Electrical Erasable Programmable Read-Only Memory (EEPROM), as well as some flash memory comprise the memory component. The RAM stores data collected from the node’s sensor and packets from the other nodes. The EEPROM store program code like RAM, but dumps its contents when power is lost. The flash memory is similar to the EEPROM except that it allows data to be written or erased in blocks instead of bytes. It can also be employed as RAM when the RAM is insufficient, but suffers significant delays and requires more power. [10]

(2) Sensors. The sensors that the nodes can employ fall into two general categories, active and passive. An active sensor positively affects its environment. It can do this by interrogating the medium to which it reacts or indicates, such as in a laser or sonar system. Passive sensors, on the other hand do not interact with their environment at all. They are merely bystanders which quantify aspects of the environment around them. These come in two varieties, omni-directional which can quantify aspects surrounding the node point, like sound, temperature, or vibration, and narrow beam which quantify direction specific aspects, like a camera. [10]

(3) Communication Device. The communication device allows the individual nodes to exchange information. Radio Frequency (RF) communication techniques are preferred for sensor networks due to the fact that no line of sight is required between the sender and receiver. This outweighs the additional complexity and expense that these techniques incur because of their need for modulation, filtering and multiplexing circuitry. Short communication distances with small information packets mean low data rates with high frequency reuse. Communication frequencies can range from 433 MHz to 2.4 GHz. [10]

(4) Power Supply. Sensor node longevity is based on its power supply. As node retrieval or replacement may be impossible and desired lifetime may be on the order of years, a node's power resources become a critical aspect of its design. Two ways to extend the life of the power source – improving battery technology and low power modes of operation for the nodes – have already been discussed. Another method to accomplish this would be to recharge the battery by scavenging energy from the environment. The use of a solar cell would be an example of this technique. [10, 16]

b. Sensor Node Operating System

The operating system controls and manages node resources, protecting access to and allowing allocation to authorized users. It accomplishes this by supporting concurrent implementation of multiple processes and facilitating communication between them. Wireless, unattended sensor networks only partially utilize this capability as they are more restricted in their code execution. The operating environment of these networks

is designed to support the more specific needs of this system, the most important of which is power management. There are several schools of thought with respect to accomplishing this: concurrent programming, process based programming, and event based programming. Event based programming seems to be the best suited for the dynamic and adaptive nature of wireless, unattended sensor networks. [10]

2. Network Topologies

Networks can be organized into a number of basic configurations which include: ring, bus, star, tree, fully connected and mesh. Figure 2 gives a general idea of how the individual points in a network are connected by each. The mesh network topology is used when implementing a wireless, unattended sensor network. Mesh networks are distributed networks in which nodes transmit to their nearest neighbor. They can easily be scaled to accommodate a large number of nodes that can be distributed over a large geographic region. The actual distribution of the mesh need not be uniform, this depiction is for ease of demonstration and only reflects the way in which the nodes communicate with each other. [17]

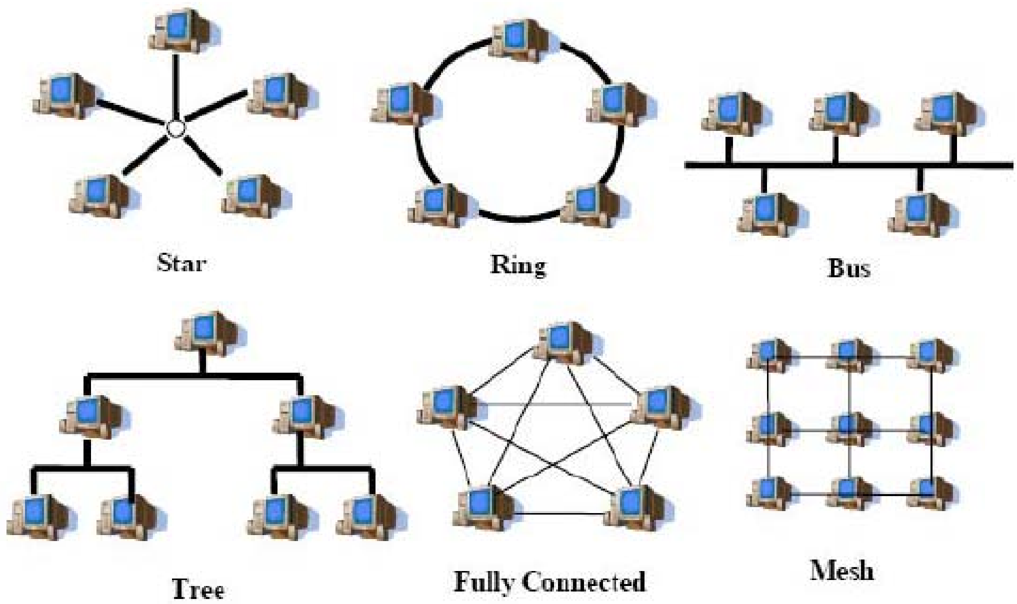

Figure 2. Basic Network Topologies (From Ref [17])

C. SENSOR NETWORK ARCHITECTURES

For the individual nodes to form a network they must be connected. It is the nature of this interconnectivity which forms the basis for the network's topology or architecture. Self-organization and low power operation are the main characteristics that govern the design of the network architecture. Both of these characteristics require distribution and decentralization in their organization. There are two general classifications into which sensor network architectures can be divided that will be discussed, they are "layered architecture" and "clustered architecture". [15, 18, 19]

1. Layered Architecture

A network with a layered architecture consists of a BS with multiple nodes that are organized into "layers". The nodes in a layer are distinguished by the number of hops required for their packets of information to reach the BS. A hop is a direct transmission link. If a node transmits directly to the BS then it is one hop away and thus in the first

layer. Each intermediate node which relays packets to the BS adds another hop and distinguishes another layer. Figure 3 illustrates this form of organization. The main advantage provided by this form of architecture is that it eliminates the need for nodes to communicate across long distances. Shorter communication distances mean lower transmission powers and greater power efficiencies. [15, 18]

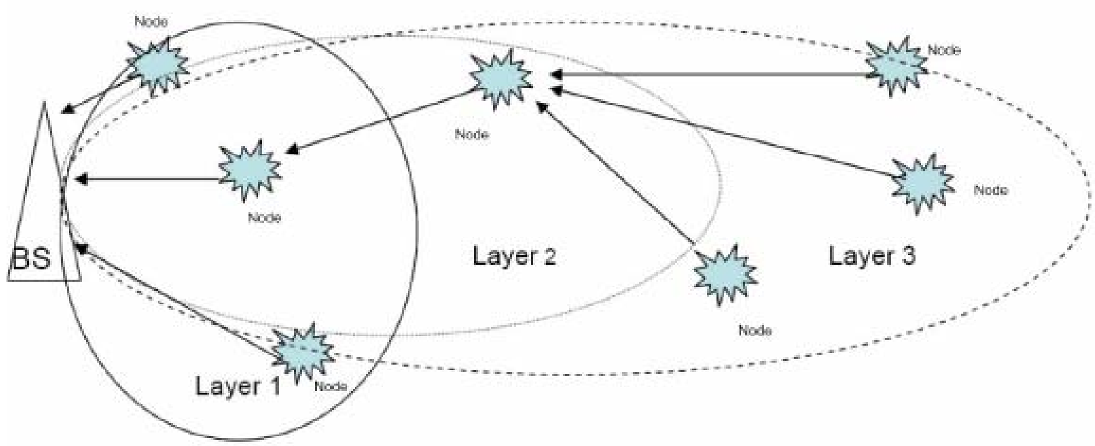

Figure 3. Layered Architecture (From Ref [5])

2. Clustered Architecture

Sensor networks with a clustered architecture consist of a BS that communicates with a number of nodes designated as cluster heads which relay all of the packets from the nodes in their cluster. The cluster head's role is two-fold. First, it coordinates all of the nodes within its cluster by facilitating communication between them. Second, it communicates outside of its cluster with the BS or other cluster heads forming the framework of the entire network. Figure 4 illustrates this form of organization. The main advantage provided by this form of architecture is that it is easily scalable and provides less of a delay in communication between nodes. Clustered architectures also excel with

data fusion applications. For this architecture to realize self-organization, the selection of cluster heads and their resulting clusters must be autonomous and distributed. [15, 19]

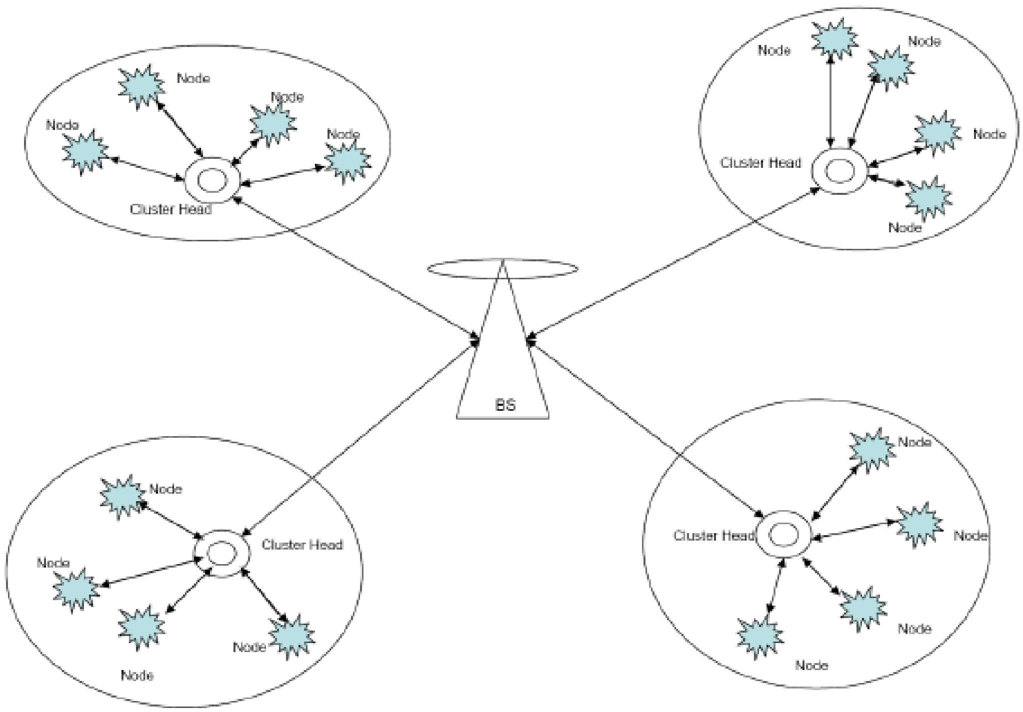

Figure 4. Clustered Architecture (From Ref [5])

D. SENSOR NETWORK PROTOCOLS

Wireless sensor network protocols also employ a layered type of architecture which is completely separate from the “layered architecture” previously discussed. Implementation of all protocol functionality in a single all-inclusive step would be incredibly difficult. The process is therefore divided into a series of separate smaller implementations which perform related subsets of tasks. These are stacked forming a layered protocol architecture which compiles all of the operations necessary for node communication. There are typically four layers associated with this form of protocol

implementation, from lowest to highest: the physical layer, the data link layer, the network layer, and the application layer. Figure 5 illustrates this form of organization. Lower layers perform more basic functions in support of the more complex functions at higher layers. The physical layer provides the basic capability of sending and receiving bits. The data link layer provides reliable transmission and reception of data, controlling information flow by maintaining fair access to the physical layer. The network layer provides the actual transfer of the information between network components. The application layer provides support for distributed applications through processes such as analog-to-digital conversion. [10, 11]

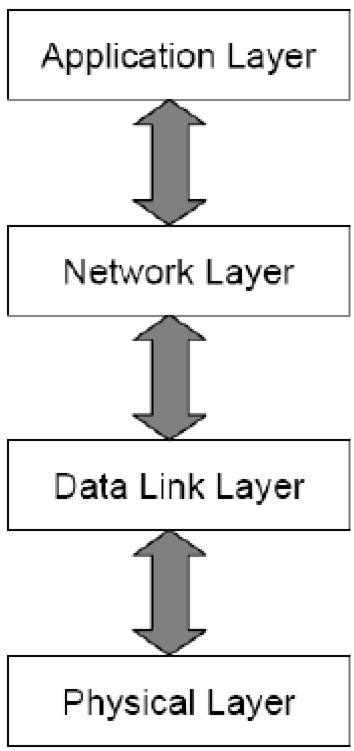

Figure 5. Typical Sensor Network Protocol Stack (After Ref [11])

1. Physical Layer

Wireless sensor networks typically utilize low bit rates. Longevity and self-organization being essential to the network's design, lower bit rates support these critical aspects. RF communications are excellent for low data rate applications and are commonly utilized in the physical layer. Communication techniques besides RF, such as infrared, are possible for use, but not desired. RF communications eliminate the need for line of sight between points of communication and are therefore preferred. [10] These techniques come in many forms. One such form is PicoRadio which uses an ultra-wide frequency band. [20] Another is Wireless Integrated Sensor Networks which uses spread spectrum techniques in unlicensed Industrial, Scientific, and Medical frequency bands. [21, 22] A final example is the Institute of Electrical and Electronics Engineering (IEEE) 802.15 Standard for Wireless Personal Area Networks which comes in three separate incarnations. The first, IEEE 802.15.1 basically represents Bluetooth technology. The second, IEEE 802.15.3 is a high bit rate implementation, while the last, IEEE 802.15.4 is a low bit rate implementation. [23]

2. Data Link Layer

The next layer is the data link layer. Its job is to provide reliable transmission of data from a source component and error-free reception of data at a destination component. This is accomplished by ensuring fair access to the physical layer. Fair access means that nodes are not given preferential access to the physical layer for any arbitrary reason, such as proximity. The main steps in this process include framing, error control, flow control, and link management. [10]

a. Framing

Framing is the process by which a transmitting node prepares an accepted data packet for transmission. Before transmission additional information, also known as overhead is added to the data packet. This overhead may include a header, trailer, or checksum which provide the receiver with information about the data in the packet and how it should continue to be processed. The checksum value is used to verify the

correctness of the data in the packet so that the receiver can send a positive acknowledgement as to the acceptance of the received frame. Power efficiency being a primary concern, framing is vitally important as packet size will affect transmission power requirements as well as the overall throughput of the network. Packet size must be optimized for the low power modes of operation required for longevity with these types of networks. [10]

b. Error Control

Noise plays a major role in any wireless medium as it can easily disrupt transmitted waveforms and therefore corrupt the desired data being transferred. Wired media are not as susceptible to the physical effects of the environment as wireless media. Effects such as reflection, diffraction, scattering, and fading make wireless media more likely to encounter errors and present considerable challenges to reliable transmission and reception of data packets. To counter some of these difficulties methods involving redundancy and retransmission of data can be employed. These measures must also be optimized to reduce their impact on overall efficiency for low power operations. [10]

c. Flow Control

Wireless sensor networks usually use a sliding window technique for flow control. This ensures that the receiving node is not overwhelmed by data packets coming in too fast for it to process. Essentially there is a predesignated window, or buffer zone at each end which stores data either waiting to be transmitted or processed. When the window is full the transmitter is forced to slow its transmissions down. With the low power operations typically desired by this type of network coupled with the low bit rates it usually employs this is not normally an issue. The sliding window method is more than adequate in addressing these requirements in most wireless sensor network applications. [10]

d. Link Management

Managing the links between the nodes of a wireless sensor network is normally handled by a medium access control (MAC) protocol. Finding, establishing, maintaining, and disestablishing the links between neighboring nodes are all part of this process. MAC is a sub-layer of the data link layer which acts as a go-between for the physical layer and the upper layers. It supports the physical layer by optimizing frame size and how often transmissions are made while supporting the upper layers by coordinating logical link control which interfaces with the network layer. All of this combines to accomplish fair sharing of physical layer medium for multiple users resulting in efficient use of the data rate. [10]

e. MAC Protocols

MAC protocols for wireless sensor networks come in three classes: fixed-allocation, demand-based, and contention-based. Fixed-allocation protocols use predetermined assignments for channel sharing. These are good for networks which traffic in continuous and deterministic data, but are inefficient for nodes with time-varying channel requirements. Demand-based protocols allocate space based on demand. These are good for networks with time-varying channel requirements, but require additional overhead for channel reservation. Nodes compete for channel access in contention-based, also known as random access protocols which requires a node to wait a random amount of time, if the channel is busy, before attempting to access the channel again. These are good for networks which propagate non-deterministic traffic, but may incur delays as collisions are an issue. [10, 15]

3. Network Layer

The network layer continues to deal with the successful transmission of data, but now within the network as a whole. The data link layer is concerned with node to node transmissions. The network layer carries this one step further concerning itself with the function of routing packets and determining data flow through the network from source to destination. With this layer the application layer requires no knowledge of any of the

underlying data transmissions or routing mechanisms. Wireless sensor networks typically employ multiple hop strategies. This means that nodes will rarely transmit information directly to its final destination, but will rely on intermediate nodes to relay data to the end component. Many techniques exist to accomplish this and they vary based on the type of architecture employed. [10]

a. Layered Architecture Routing Techniques

Flooding, gossiping, and controlled flooding are routing techniques typically used for layered architectures which center on a BS. The simplest form is flooding which forwards packets to all neighbors ensuring that the packet will reach its destination as long as it is in the network. Packets are forwarded only once to prevent infinite regeneration and a time-out feature is employed to prevent infinite propagation of packets. Implementation is simple, but results in multiple duplications which hamper efficiency. Gossiping is another approach which minimizes packet duplication, but continues to inhibit efficiency as it incurs substantial delay times for packets reaching their destinations and offers no reliability. In this technique nodes only forward packets to a single random neighbor in the hopes that it will reach its destination. Combining these two techniques results in controlled flooding. Here nodes forward packets randomly to a number of available neighbors which can help to optimize network performance. [10, 15]

All of these are easy to design and implement, but perform poorly in terms of packet transmissions and receptions and delay. These performance issues can be somewhat resolved through the use of a routing table. Routing tables associate cost values with nodes based on their suitability for relaying packets and choose the least expensive path. Packets can then be transmitted without duplication or delay. Routing tables can be either table driven or on-demand. These only differ in that table driven maintain routing tables all the time, while on-demand build them only when required for transmission. [10, 15]

b. Clustered Architecture Routing Techniques

In a distributed network, where peer-to-peer communication is desired rather than all queries originating from a BS, more sophisticated routing techniques become necessary. One such approach is to use a directed diffusion routing protocol which allows destinations to specify data rate requirements using interest gradients. Data rates are increased or decreased based on the application's ability to deliver packets of interest. [24]

Other routing approaches for peer enabled wireless sensor networks include: Sensor Protocols for Information via Negotiation (SPIN), the cost-field approach, and the Geographic Hash Table (GHT). SPIN refines the flooding technique by improving the versatility of resources through negotiation. This negotiation prolongs network longevity by reducing duplication and the overlap caused by it. The cost-field approach uses a step-wise algorithm to determine the most efficient path from source to destination. Packets contain a cost-so-far field which is updated at each intermediate node. With each step the algorithm chooses the node associated with the least cost to proceed through the network. For GHT keys are hashed into a set of geographic coordinates. A key-value pair is then established for a node close to the position of its associated key. Mapping consistency ensures proper data routing and distribution among nodes using a balanced scalable scheme. [25-27]

Power constraints being of paramount interest for wireless sensor networks, routing protocols have been developed which consider efficiencies outside of the network layer. Efficiencies at every level of the sensor network protocol stack depicted in Figure 5 are considered for protocols gaining the widest acceptance. Two such protocols are Low-Energy Adaptive Clustering Hierarchy (LEACH) and XMesh. LEACH optimizes energy efficiency by rotating the position of cluster head between the nodes in a cluster. Cluster heads by the very nature of their operation consume the most power and spreading this responsibility around equalizes node energy expenditure. XMesh evolved from earlier developments of Hill and Woo, the Surge-reliable and Mint Route protocols. XMesh will be discussed in greater detail later in this thesis. [28, 29]

4. Application Layer

For wireless sensor networks, the sensor is the application layer. That is to say that the applications being supported by this layer are those of the sensor. Essentially, the physical phenomena sensed from the environment are converted into data suitable for transmission. The physical quantity, which is typically analog, is sampled and converted into a digital signal. This signal is then formatted into a packet and framed for transmission to its designated destination. This layer represents the logic necessary for supporting any sensor applications. [10, 11, 15]

E. WIRELESS NETWORK CHALLENGES

Many challenges are involved in the use of wireless sensor networks. With most applications involving some manner of inaccessibility, the primary design concern for any implementation hoping to last any finite amount of time is power. Power conservation must be considered for every aspect of sensor node design and operation. A certain amount of flexibility and autonomy is also desired so that the system can be adapted and adapt to dynamic environments. Finally, for the network to be truly effective security measures must be considered to ensure that the information received from it is accurate.

1. Energy Management

Energy management can be accomplished for a wireless sensor network in a number of ways. Optimization of every aspect of a node’s design should apply the most stringent energy constraints allowed by the threshold of performance required by the application. Data transmission being the largest power drain, most design features will focus on streamlining this process. This can be achieved in a variety of ways ranging from choosing the appropriate carrier frequency to node deployment and data handling.

a. Transmission Medium

The choice of transmission medium is important for wireless sensor networks. Radio, infrared, or optical methods can be used to form the basis for the

network. Infrared and optical communications require a direct line of sight between source and receiver, whereas radio communications do not. It is for this reason that radio communications are typically chosen for wireless sensor networks despite their problems associated with fading and higher error rates which may affect network routing operations. Choosing the proper frequency band is also very important. Carriers in the ultra-high frequency (UHF) range have been determined to be most advantageous due to certain hardware constraints as well as antenna efficiency and power consumption rates. [10, 30]

b. Node Deployment

Deployment of wireless sensor network nodes depends on the application and can be accomplished randomly or deterministically. When deployed randomly, a non-uniform distribution may be created requiring an ad-hoc infrastructure. When deployed deterministically, data routing can be accomplished along a pre-determined path as nodes are placed manually. [31] Regardless of the method, node deployment and distribution must take into consideration coverage and connectivity. A node's coverage capability is based on its sensing range, the limited physical area of the environment that it can monitor. Node connectivity is based on its ability to relay the information that it has collected back to the base station via the network. An area is completely covered if the radio range of a working connected node is at least twice that of the node's sensing range. It is therefore desired for nodes to be deployed in high density to shorten transmission distances, preclude them being isolated and thereby prolong network life. [32]

c. Data Aggregation

Due to the desired proximity that deployed nodes share, redundancy of information within the wireless sensor network is likely. In order to minimize this inefficiency, data from multiple nodes sensing the same event can be combined or aggregated together. This aggregation can be a function of a number of factors, such as maxima, minima, or averages. [33] Since data processing consumes less energy than

transmission, data aggregation can greatly improve energy efficiency. Signal processing techniques like data fusion are another method of data aggregation. Nodes can produce more accurate output signals through techniques such as beam forming to combine incoming signals, reducing noise. [28] Localization and synchronization can be used to enhance data aggregation.

(1) Localization. Localization is the process by which a sensor node can know its location specified either globally or relatively. A node's global location represents its actual position on the earth which can be determined using Global Positioning System satellites (GPS). A node's relative position does not refer to a particular position on the earth, but rather its position in relation to the other nodes in the network. GPS is not typically used in wireless sensor networks as it is bulky and has high power requirements. Most localization techniques employ beacon nodes which either transmit or receive beacon signals depending on exterior or interior use respectively. Distances between nodes are then estimated based on beacon signal strength. Directionality is determined using assumptions that beacon nodes broadcast to all nodes in the network while pivoting at a continuous angular velocity based on a central controller. [15, 34, 35]

(2) Synchronization. For synchronization to occur, all nodes must agree on a single standard time. Synchronization algorithms fall into two different categories: long-lasting or global synchronization and short-lived or pulsed synchronization. In one global synchronization scheme a node leader is elected with knowledge of neighboring nodes' control signals. The leader transmits synchronization messages periodically to neighboring nodes which are rebroadcast throughout the network. [36] In an example of a low power synchronization scheme, a broadcast beacon transmits a synchronization message to normalize all node time-stamps in order to observe an event. This creates a pulsed synchronization for the nodes within transmission range of the beacon. In dynamic networks where topology changes or mobility are factors, resynchronization is required to keep node clusters on a universal clock. If two clusters merge due to mobility, the node chosen as network coordinator updates the clocks of each member of the newly formed cluster to match its own. [15, 37]

2. Scalability

Depending on the application sensor nodes could number into the thousands with individual nodes possessing independent sensing, computing, and wireless communicating capability. During normal operations most nodes will be inactive with a few providing a broad overview of the environment until a sensing event is triggered. Routing algorithms must be capable of handling multiple triggering events among such a large number of nodes simultaneously. [12] This scalability is important not only as the number of nodes grow, but as they shrink. Fault tolerance is the sensor networks ability to sustain uninterrupted functionality in the event of node loss or failure. Node failure can occur for a number of reasons, such as physical, power failure, or environmental or man-made interference. [38] Routing protocols must also be able to contend with multiple nodes failing. This may involve establishing new links, varying signal rates or transmitting powers on existing links, or rerouting paths to the base station collecting the data all the while considering power consumption. Any combination of these methods may be necessary in redundant layers for adequate fault tolerance based on application specific requirements. [12]

3. Security

Sensor network security is important due to the trust level associated with event detection and the credibility afforded the aggregate data in the decision making process. The very nature of a wireless sensor network constrains the techniques typically established for security measures. Assuring data authentication and integrity avoid message forgery and alteration respectively. To accomplish these while maintaining privacy are paramount in developing effective security measures. [14, 15, 25]

Wireless sensor networks can come under attack in a number of ways. Since nodes propagate messages through the network by repetitive forwarding with broadcasts they can be vulnerable to forwarding attacks. These types of attacks are intentional and cause a node to forward packets in a manner other than would be specified by its protocol, if at all. In “sinkhole” attacks, nodes give false representations for the most efficient route through the network. Another form of attack is a replay attack. Replay

attacks are reintroductions of old packets as new messages. These can be prevented by having the message packet carry a counter value. Wireless sensor networks also require semantic security. This prevents adversaries from deciphering text message contents even after observing multiple encrypted versions of the same message. These can also be prevented by having the message packet carry a counter value. [15, 25

High processing requirements make symmetric or key cryptography techniques undesirable for use with low power sensor network applications. An asymmetric method must therefore be used for data authentication. With adequate processing power, Localized Encryption and Authentication Protocol (LEAP) or Intrusion Tolerant Routing in Wireless Sensor Networks (INSENS) can be used. Consisting primarily of two components, sensor network encryption protocols (SNEP) and a micro-version of the timed, efficient, streaming loss-tolerant authentication (μ-TESLA) protocol, Security Protocols for Sensor Networks (SPINS) offer a number of excellent techniques for sensor networks with limited resources in particular. With the additional overhead of only eight bytes per message, SNEP provides data authentication, replay attack protection, and semantic security. The μ-TESLA protocol assures the identity of the sender by ensuring broadcast authentication. [15, 25, 39 - 42]

F. WIRELESS NETWORK APPLICATIONS

A wide variety of sensors can be employed for wireless sensor networks to monitor an equally wide variety of parameters. Employing thermal, infrared, acoustic, magnetic, or seismic sensors nodes can detect temperature, lighting, noise or movement conditions discretely by event or continuously for trend information. These indications can provide information ranging from alarms that merely grant awareness to automatic control of actuators. [6]

1. Commercial

Heating ventilation and air-conditioning (HVAC) is a costly and unavoidable expense. Climate control in commercial buildings is an important consideration that can affect employee productivity and product quality. The system is typically centrally

controlled by a limited number of thermostats and humidistats primarily due to wiring costs. This can lead to severe inefficiencies in implementation simply because of a lack of information completeness. Rooms or even parts of rooms could be too hot or cold compared to others for no other reason than lack of information. Wireless sensor networks could provide more complete information at a reduced cost for more efficient operations. Air temperature and flow could be automatically monitored and controlled for maintenance of not only the environment, but the equipment providing the environment. Optimizing system performance could lead to yearly cost savings in the tens of billions of dollars and carbon emission reductions in the tens of millions of tons. [6, 16]

Sensor nodes can also be utilized for control of inventory. By attaching appropriate sensor nodes to inventory items any number of qualities about the item can be monitored. These can range from the items' mere presence and number to their exact location or from the condition of their environment to how long they have been there. [6]

2. Industrial

Large industrial complexes can have a number of plants each with a number of control and monitoring stations which provide indications for a number of plant conditions. Again wireless sensor network options provide an inexpensive option to the wired environment. The sensors, control devices, and actuators are inexpensive for either option, but the wired environment requires cable shielding to protect signal integrity and accuracy. This represents the greatest cost savings as plant conditions often change slowly enough that wireless means can meet the low data throughput requirements with high reliability. [6]

3. Environmental

Monitoring environmental conditions can be very important for a variety of applications. Many agricultural markets can use wireless sensor networks to monitor crop conditions ranging from soil moisture and nutrient content to temperature, humidity, and potential pest concerns. They provide an inexpensive way to cover a large area very

thoroughly with the potential for automatic response to certain key conditions. This is well suited for vineyards as minor changes can have a tremendous effect on the value of a crop. [6]

Monitoring seismic activity is important in the tracking of numerous natural conditions that may lead to disaster, such as earthquakes, tsunamis, or volcanic eruptions. Timely receipt and analysis of this type of data could be instrumental in evacuation of potentially affected areas and the saving of potentially innumerable lives. The wireless and low power nature of these systems makes them ideal for remote implementation over long periods of time at minimal cost. [6]

4. Military

Military applications are a natural extension of this capability. The ability to monitor both friendly and enemy forces and their positions and movements is an integral part of military Command, Control, Communications, Computing, Intelligence, Surveillance, Reconnaissance, and Targeting (C4ISRT) system. Understanding available assets and their locations can be just as important as knowing enemy strength and position and wireless sensor networks provide an easy method for tracking both. Maintaining an inventory of your own force structure can be accomplished in much the same way as in commercial applications. Wireless sensor networks also provide an unobtrusive way to monitor remote areas of a battle-space without the need to risk the physical intrusion of troops into an unknown situation. This completeness of information can allow a commander to respond to situations in the most appropriate manner. [6]

G. SUMMARY

The purpose of this chapter was to provide an introduction to wireless, unattended sensor networks. Beginning with the basic components that comprise the wireless sensor network, some basic concepts that apply to network networks in general were discussed. From this point certain aspects of overall network architecture were brought up which

lead to discussion of the protocols that are used to implement them. This was followed by bringing to mind some of the challenges associated with employing this type of sensor network for the various applications that followed.

III. EXPERIMENTAL WIRELESS SENSOR NETWORK

A. CHAPTER OVERVIEW

This chapter continues to discuss topics related to wireless sensor networks and their constituent components, but this time with more focus towards the wireless, unattended sensor network that was used as a part of the experiments performed for this thesis. The specific components that were used were manufactured by Crossbow Technologies along with the operating system, TinyOS, and the routing protocol, XMesh are described. This is followed by a brief discussion of previously completed research that also involves wireless sensor networks that employ the same technology.

B. SENSOR NETWORK COMPONENTS

Sensors, transceivers, and gateways are the basic components of the wireless sensor network. The sensors, transceivers and gateways employed in this research were manufactured by Crossbow Technologies. The sensor nodes in a wireless sensor network are often referred to as "motes" and will heretofore be referred to in the same manner. These motes are a readily available commercial off-the-shelf product. The hardware and software platform provided combine sensing, communications and computational capabilities into a single package. The hardware design consists of a mote processor/radio (MPR) and a mote sensor board (MTS). The MPR board has a small low power radio, processor, A/D converter and battery. The MTS can have one or more sensors integrated onto a single board. MPR and MTS boards can be combined in many ways. The two types of boards combine to create a complete sensor mote capable of performing all of the functionality necessary to form the wireless sensor network. Conforming to low-power operating requirements for longevity, the complete mote typically consumes 100 mW while active and 30μW while idle. [43]

The wireless sensor network components are depicted in Figure 6 demonstrating their functionality and connectivity. A personal computer (PC) can program the sensor mote in one of two ways. This can be accomplished through a gateway interface as

shown in Figure 6 or through the air by the operating system, TinyOS using a component called Deluge. The sensors are run by the application programs which pass sensed data to the microcontroller. The microcontroller can allow reporting based on time or by exception. With reporting by exception the microcontroller only reports an event when a query of interest was cached. The data is then passed from the microcontroller to the transceiver for wireless communication. The transceiver then forwards the packet to a peer or the BS that is in radio range once clear channel estimation and recognition is complete. Finally, the sensed data is received by the BS which forwards it to the PC for processing and analysis. [29, 44]

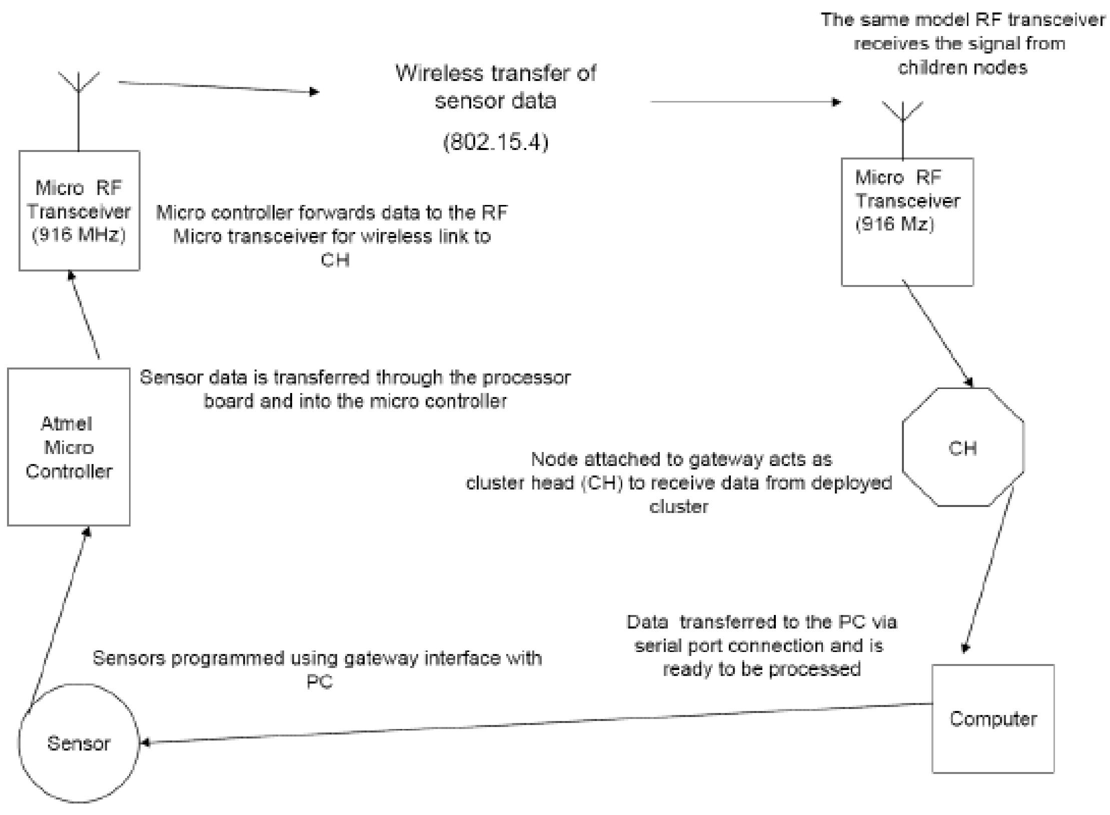

Figure 6. System Block Diagram of a Mica2 Mote (with description of each functional block). (After Ref. [44].)

1. Crossbow Technologies' Transceivers

Crossbow transceivers range from 2.4 GHz which follows the IEEE 802.15.4 standard down to an operating frequency of 433 MHz specific to the market in the United States. A variety of designs allow communication at frequency bands at 915 MHz and 2.4 GHz. With the same power output the 433 MHz band operates with the longest range utilizing four channels spaced with 500 kHz between them. Operating between 902 MHz and 928 MHz, the 915 MHz band has forty-eight 500 kHz bandwidth channels also spaced with 500 kHz between them. With worldwide acceptance and a larger bandwidth, the 2.4-GHz band uses sixteen channels defined specifically by the IEEE 802.15.4 standard. [29, 45]

Mote construction and functionality depend entirely on the frequency band that will be utilized. Crossbow motes are more often recognized by their trade names MICA, MICA2, MICA2DOT and MICAz. The subcomponents of the Crossbow Technologies "MICA" family of motes are detailed in Table 1, comparing the specifications and features of their respective technologies. All MICA motes utilize the same subcomponents with the only exception being the MICAz which employs a slightly different radio. Longevity being the governing principal in mote design, the individual components will be discussed in more detail. [29, 45]

Table 1. Specifications of the Four Different MICA Subcomponents. (From Ref. [45].)

Mote Hardware Platform		MICAz	MICA2	MICA2DOT	MICA
Models (as of August 2004)		MPR2400	MPR400/410/420	MPR500/510/520	MPR300/310
MCU	Chip	ATMega128L			ATMega103L
	Type	7.37 MHz, 8 bit		4 MHz, 8 bit	4 MHz, 8 bit
	Program Memory (kB)	128			
	SRAM (kB)	4			
Sensor Board Interface	Type	51 pin		18 pin	51 pin
	10-Bit ADC	7, 0 V to 3 V input		6, 0 V to 3 V input	7, 0 V to 3 V input
	UART	2		1	2
	Other interfaces	DIO, I2C		DIO	DIO, I2C
RF Transceiver (Radio)	Chip	CC2420	CC1000		TR1000
	Radio Frequency (MHz)	2400	315/433/915		433/915
	Max. Data Rate (kbits/sec)	250	38.4		40
	Antenna Connector	MMCX		PCB solder hole	
Flash Data Logger Memory	Chip	AT45DB014B			
	Connection Type	SPI			
	Size (kB)	512			
Default power source	Type	AA, 2×		Coin (CR2354)	AA, 2×
	Typical capacity (mA-hr)	2000		560	2000
	3.3 V booster	N/A			✓

2. Radio

The most important component of the MPR board is the radio. It provides the capability for sharing real-time information throughout the wireless sensor network. Crossbow MICA, MICA2, and MICA2DOT motes use a Chipcon CC1000 RF transceiver. Complementary Metal-Oxide Semiconductor (CMOS) technology is utilized by this device which requires low power for operation. Supply voltage in the range of 2.1 V to 3.6 V and transmit current requirements at 9.1 mA are key low power features. A single-chip RF transceiver and programmable operating frequencies are other included features. A Phase Shift Keying (PSK) modulation scheme and an integrated bit synchronizer are employed for transmission and reception with a data rate of up to 76.8 kbps. A dedicated bus architecture is used to configure the radio registers and the Serial Port Interface (SPI) bus dedicated to them for data transfer. The radio itself possesses no buffering capability which requires timely delivery of bits to the processor. Crossbow MICAz motes use the Chipcon CC2420 RF transceiver. This device also follows the IEEE 802.15.4 standard, but was designed to meet the specifications of the Zigbee

alliance as well, assuring worldwide acceptance in the 2.4 GHz band. Looking at the MICA, MICA2, and MICA2DOT motes side-by-side with the MICAz motes in Table 1, a comparison of the transceiver chip capabilities can be made. The difference in features between the CC1000 and the CC2420 are a 17.4 mA transmit current and a Direct Sequence Spread Spectrum (DSSS) modem with 2 Mchips/sec capable of data rates up to 250 kbps. [29, 46]

3. Microcontroller

All Crossbow motes use the Atmel ATMega128L microcontroller except the MICA which uses the ATMega103L as indicated in Table 1. The ATMega128L employs a 7.37 MHz clock (4 MHz for MICA2DOT), 128 kB of flash memory, 4 kB of Static Random Access Memory (SRAM) and two Universal Asynchronous Receive and Transmitters (UART). It uses two busses, an Inter-Integrated Circuit (I2C) bus for communication with switches and a SPI bus for communication with the radio. Constrained by 4 kB of memory; this device was given special consideration while developing the operating system. The amount of SRAM and the efficiency with which it estimates and employs memory are advantages of this device over others on the market. The processor offers two modes for sleep operating: idle and power-save. The idle mode shuts the mote down while power-save shuts the mote down with the exception of an asynchronous timer which continues to run. The ATMega128L can awaken from either of these sleep modes in fewer than 200 msec or in fewer than 1 μsec if it is set up to use an internal oscillator. With sleep mode current as low as 1μA, power can be delivered by two AA batteries. These provide a 3 V source whose operating voltage can be as low as 2.2 V. The MICA2DOT is powered by a 3 V lithium coin cell battery, providing a capacity of 560 mA-hrs. [29, 47 - 49]

4. Gateways

Gateways allow the network to interact with devices outside the IEEE 802.15.4 standard and provide the functionality for data storage and analysis. Removing this burden from the mote supports low-duty-cycle operation thus improving network

longevity. Crossbow Technologies produces a number of gateways for use with their motes which include the MIB510, the MIB600 and the Stargate. The MIB510 and MIB600 gateways require interface directly with a PC while he Stargate gateway interfaces remotely using the IEEE 802.11 standard for access. The gateways are cluster heads that can establish peering relationships and parent-child relationships and scale to network topology. [48]

The MIB510 gateway connects via an RS-232 serial port that it shares with the mote to allow it to be programmed and provide BS operations. The MIB600 gateway allows for multiple operations via an Ethernet port like providing power and remote code debugging over Transmission Control Protocol/Internet Protocol (TCP/IP) on top of the capabilities of the MIB510. A mote acting as the network coordinator must be connected to the MIB510 or MIB600 to forward data outside of its coverage area. Motes acting as sensors in the network are designated by node identifiers (ID) to distinguish their data. These gateways require dedicated PCs for users to access and translate their data. [48, 49]

When a sensor network requires remote operability or a dedicated PC is unfeasible, the Stargate gateway allows remote access using the IEEE 802.11 standard. This can be accomplished via a Personal Computer Memory Card International Association (PCMCIA) card slot or by connecting to a Global System for Mobile communication/Code Division Multiple Access (GSM/CDMA) mobile phone network. This gateway provides an increase in processing power, employs the Linux Operating System (OS), and is compatible with all MICA motes. It also has additional slots for extra memory, a PCMCIA card, as well as a transceiver utilizing the IEEE 802.15.4 standard. TCP/IP connections or mobile phone networks are used to facilitate remote access and data retrieval. The Stargate increases functionality by easing constraints on form factor, processing power and energy consumption while significantly improving the network scalability. [48, 49]

5. Other Components: Memory, Interfaces and Ports

All of the MICA motes employ 512 kbytes of flash memory. This is attached to a UART port for data logging and over-the-air programming. Storing data to memory

consumes 15 mA which negatively impacts battery life. An analog-to-digital conversion interface is provided by a fifty-one pin expansion connector on the MICA2 and MICAz. The expansion connector provides numerous interfaces including eight 10-bit analog input/outputs and twenty-one general purpose input/outputs. There are also interfaces for power and ground, control of peripheral sensor power, and sensor output data analog-to-digital conversion. UART interfaces and an Inter Integrated Circuit (I2C) interface round out the expansion connector. The analog-to-digital conversion interface on the MICA2DOT has nineteen pins with six 10-bit analog input/output ports and six general purpose input/outputs. All motes have an interface for Data Input Output (DIO) and a Multimedia Communication Exchange (MMCX) connection for the antenna. [49]

6. Sensors

Sensor subsystem composition is entirely application dependent and connects to the mote via a fifty-one pin expansion connector. MTS310 sensor boards have a variety of sensing modalities with the following sensing options: acceleration, magnetic field, acoustic, temperature, and light sensors. The boards are also equipped with a sounder that is used for the purpose of localization. Figure 7 shows the MTS310 with its component sensors labeled. [43]

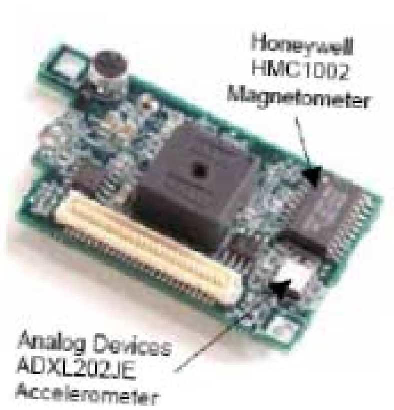

Figure 7. MTS 310 Sensor Board with Honeywell HMC1002 Magnetometer and Analog Devices ADXL202JE Accelerometer. (From Ref. [43].)

C. SENSOR NETWORK OPERATING SYSTEM

The strict application requirements that wireless sensor networks present place unique demands on their software components to compliment their system's hardware components. Most of the challenges in developing sensor network devices revolve around embedding the software into the sensors. The software must balance maintaining enough agility for simultaneous use of system resources, such as computation and communication, while making stringent use of the processor and its associated memory to conserve power. The Tiny Micro-Threading Operating System (TinyOS) software is a small operating system that supports wireless sensor networks and standardizes the development of applications and creation of extensions for the hardware. The framework for the experimental wireless sensor network used in this thesis combines portions of the IEEE 802.15.4 standard with TinyOS. TinyOS and its associated programming language nesC are described below. [50]

1. TinyOS

To provide the desired levels of operating efficiency TinyOS uses an event-based execution scheme. High levels of concurrency can be managed using a small amount of memory with this execution scheme. Hardware events, those caused by a timer, sensor, or communication device, are interrupts that are rapidly executed along with all associated tasks. Tasks are executions that run in the background without disturbing concurrent events and can be scheduled at anytime. These executions are always deferred until completion of current events that are still pending. When the processing of all events and their associated tasks are complete, completion must be declared by the application to allow the processor to enter a sleep state, rather than remaining active waiting for other events. [50]

As a system TinyOS is organized into two main areas of concern, the first of which are its associated components. Higher level components must declare the commands that they will use as well as the events that they will handle. Lower level components must declare the commands that they will accept as well as the events that they will signal. Commands are issued from higher level components to lower level

components and initiate action in the lower level. Events are signaled from lower level components to higher level components and notify higher levels that an action has occurred. Each module's interface has associated commands and events that comprise it. The declaration made by each component regarding the use or acceptance of commands and the signaling or handling of events facilitates modularity. Commands are prohibited from signaling events to avoid cycles of commands and events. This allows the application to dictate the wiring of components and allocation of memory. Commands and events are each intended to perform small fixed amounts of work that occur within the context of executing a thread. A thread is a single sequence of instructions that executes quickly and runs to completion. They are called by commands to lower level components and generate events to higher level components during execution. In this way TinyOS deals with memory constraints by reducing redundancy thus conserving memory. [12, 50]

The second portion of TinyOS's overall organization is comprised of a scheduler. A two-tier scheduler that utilizes a length seven, first-in-first-out queue is employed. One of the tiers is for events – the higher priority items – while the other tier is for tasks – the lower priority items. Events have the ability to preempt a task, but cannot stop its accomplishment. [12, 50]

Discussion of the interactions within a node will be driven by the execution of the application. Several networked nodes within communication range of each other that will periodically transmit their measurements via the network will constitute the application. Routing information is programmed into the network nodes all of which possess peer-to-peer routing capability. Figure 8 depicts the internal components of the described node. [12, 50]

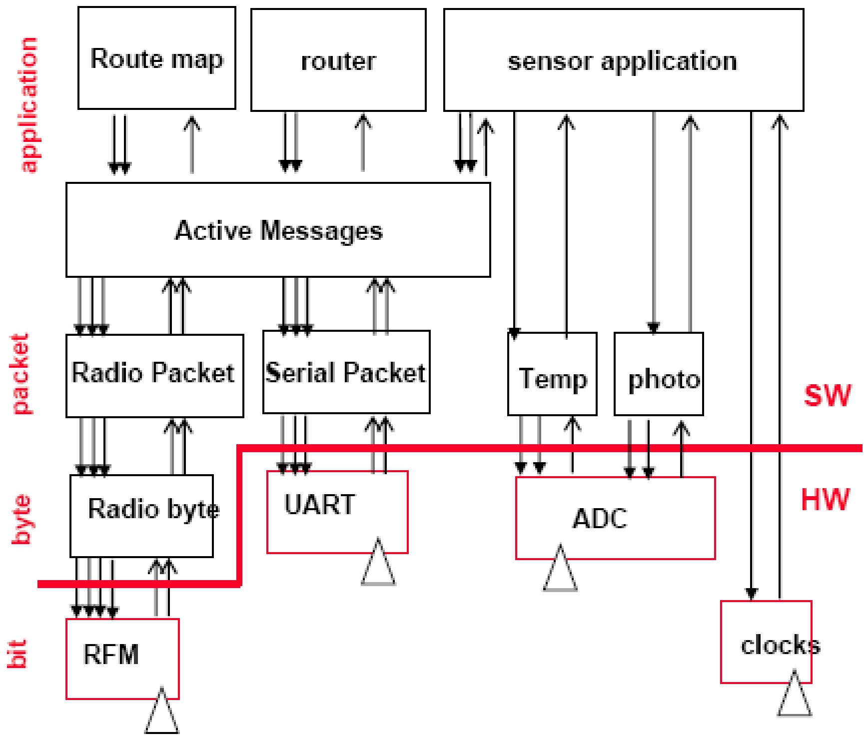

Figure 8. TinyOS Component Interfaces for a Multi-hop Sensing Application. (From Ref. [29].)

The purpose of the application is to service the network and the sensors that make it up. The application layer ties together vertical component stacks that are used to represent each of these input/output devices. Data from the application is transmitted as an active message of a fixed length. Each active message contains an identified handler. In the network layer appropriate handlers are implemented upon message arrival. For the application this is analogous to events being signaled. For intermediate nodes receiving packets between the BS and the destination, message handlers begin the process of retransmission. Once packets reach the BS message handlers forward them for execution. Timer events are employed to periodically begin collection of data during execution. The application executes the "send_message" command to begin transferring sensor data once data collection is complete. This command records the location of the message and schedules a thread for direction of the transmission. Once executed, threads assemble the

packets and begin a string of commands. By calling the “TX_byte” command within the Radio Byte component byte-by-byte transmission commences. When this transmission is completed, the “TX_bit_evt” is transmitted to the packet level controller by the Radio Byte component through the “TX_byte_done” event. Once transmission of all of the bytes in a packet is complete, the “TX_packet_done” event is cued by the packet level controller. This event is propagated in turn to the application through the “msg_end_done” event. [50]

There are times when the node is active, but no transmissions are occurring. In these instances the Radio Frequency Modulator (RFM) component will signal the Radio Byte component upon detection a start sequence. This will reserve the transmission process at which time components will convert the bits into bytes and then frame the bytes into packets. Each component will actively signal the higher level once a packet is assembled. Once the address is verified and a local address match is found the appropriate message handler is implemented. [50]

2. nesC: a Programming Language for Embedded Systems

The nesC programming language is what TinyOS, its libraries and applications are written in. It is a new language for programming structured component-based applications that is primarily intended for embedded systems, such as wireless sensor networks. Similar to C, the syntax of nesC supports the TinyOS concurrency model. It also allows for robust network components to be formed through the use of mechanisms for structuring, naming, and linking together software components. These can be easily composed into systems that are complete and concurrent. [50]

D. XMESH ROUTING PROTOCOL

Crossbow Technologies developed the XMesh routing protocol to run in the TinyOS environment [51] on the MICA family of motes. It is a multi-hop, ad-hoc mesh networking routing protocol that is capable of autonomous network formation with no need for human intervention. It is also adaptable enough to automatically add and remove network nodes without the need for a network reset. A routing beacon from the BS is

used for establishing packet return routes. The general acceptance of Crossbow motes for research purposes made them an obvious choice for use in this thesis. This section will provide a greater understanding of the XMesh multi-hop routing protocol used by the motes in the wireless sensor network evaluated. [52]

1. Protocol Components

Figure 9 depicts the high level component interactions and how implementation of the routing protocol is accomplished. The protocol uses a routing beacon from the BS for establishing packet return routes. Inbound link quality (i.e., reception quality) estimates are maintained by each node. Since the routing protocol is based on the outbound link quality (i.e., transmission), these are propagated back to their neighbors. [6, 53]

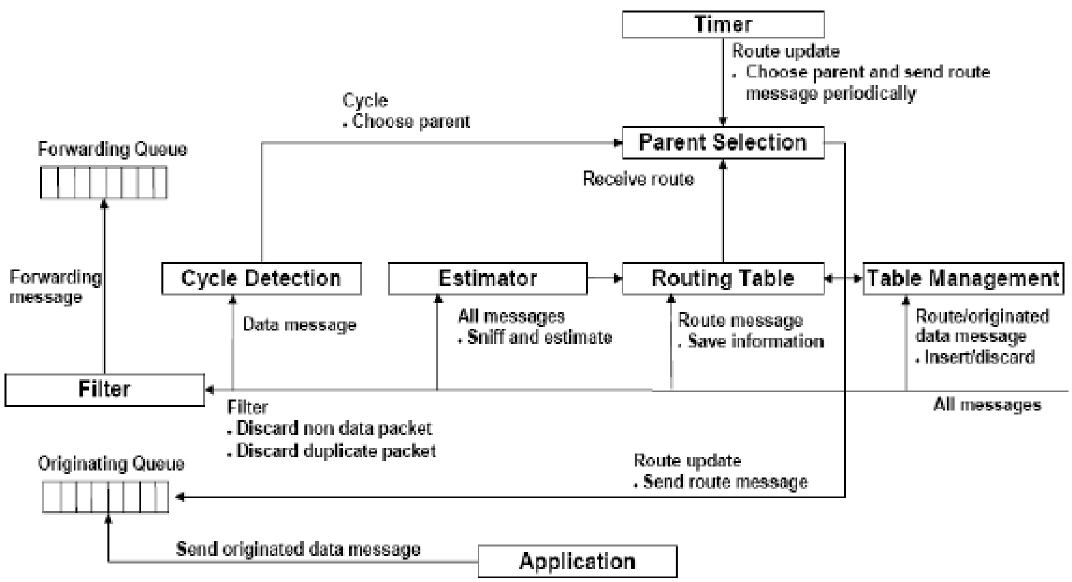

Figure 9. XMesh Routing Components. (From Ref [53])

a. Routing Table

Each routing table contains up to sixteen entries with the status and routing information for its neighbors. It includes fields containing the following: the MAC address, an estimated routing cost to the sink, a parent address, a child flag, a list of inbound link qualities, an outbound link quality, and data structures for link estimation. [6, 53]

b. Estimator

The link qualities of neighboring nodes are computed by the estimator. Link quality is a measure of the packets sent via a given link that arrive complete and intact. It is determined by expressing the ratio of received packets to expected packets as a percentage. Another way to view this would be as the packet delivery success rate. Hop count and route stability are other ways to measure link quality. [6, 53]

The estimator monitors packets in the channel and observes packet success and loss events to produce estimates of link quality. These estimates can be used by higher level protocols to build routing structures. The estimator must be able to react quickly and appropriately to changes in link quality. A balance between rapidly responding to large fluctuations in link quality and maintaining stability when those fluctuations turn out to be short term must be achieved. Rapid response capability will enable greater adaptability for higher-level protocols to environmental changes and mobility. Limited memory and computational ability require that it not utilize significant storage and processing resources. XMesh uses a Window Mean with an Exponentially Weighted Moving Average (WMEWMA) for estimating link quality. The success rate over a fixed period of time is calculated and the average is smoothed with an Exponentially Weighted Moving Average (EWMA). [6, 53]

c. Table Management and Timer

Table management policy determines the insertion, eviction, and reinforcement of node information in the routing table. When a node receives packets, it

performs neighbor discovery by recording information about the nodes from which the packets were received. An estimate of link quality is used to determine whether or not the node should be considered as a neighbor. Neighbor analysis is performed for each incoming packet from a source for insertion or reinforcement consideration. If the source is already represented in the table, it may be reinforced in order to maintain its presence. If the source is not present and the table is not full the source is inserted. If the source is not present and the table is full, the node must decide whether to discard the information associated with the new source or to evict another node from the table in order to insert the new source. This process occurs either as a result of passive monitoring or active probing. A timer is used to trigger such events as this active probing for the periodic update of routing tables, as well as messaging and a few others. [6, 53]

d. Parent Selection

Parent selection occurs periodically to identify a neighbor as a potential parent for routing purposes. A node's cost is an abstract representation of its distance to the BS or sink. Its basis can stem from various metrics such as the hop count, the number of transmissions, or the number of reconfigurations over time. A neighbor will only be selected as a potential parent if the cost of the current node becomes greater than its own. A neighbor may also be considered as a potential parent to replace an existing parent if the quality of its link drops below a certain threshold, if the sink becomes unreachable through the existing parent, or if a cycle is detected. When the connectivity through an existing parent degrades, its link quality estimate will decline over time and necessitate the selection of a new parent. If the connectivity to the current parent degrades completely with no new potential parents available, the node declares that it has no parent and assumes a cost to infinity. If parent changes become too frequent the network will become unstable due to routing fluctuations. Routes therefore undergo evaluations on a periodic basis rather than when route updates are received. [6, 53]

e. Cycle Detection

A cycle occurs when a node originates a message and it returns. This will occur if the message has been forwarded to another child instead of a parent. Neighboring child nodes can be identified by monitoring their forwarded traffic. The messages from a neighboring child will contain their parent's address and they will not be considered as potential parents. Cycles can be detected quickly because each of the nodes can act as a data source and as a router. Once detected, a cycle is broken by the node replacing its existing parent with a new one or by declaring that it has no parent and assuming a cost of infinity. [6, 53]

f. Filter

The filter removes any unnecessary packets, including duplicate packets and non-data packets. With no filter there will be more retransmissions as duplicate packets continue to be forwarded possibly causing more contention. This inefficiency in energy management can not be afforded with the constrained resources of this system. An event as simple as a lost acknowledgement can create duplicate packets when the originating node retransmits the packets it believes was not received. Duplicate packets are avoided by appending the identifier of the sender and the originating sequence number to the routing header. This is accomplished in the routing layer at the originating node. The identifier and originating sequence number of the most recent originator are retained by each parent in child entries in the routing table. This suppresses the forwarding of duplicate messages. [6, 53]

2. ROUTING ALGORITHM

The XMesh routing algorithm uses a Minimum Transmission (MT) cost metric. This cost metric minimizes the total number of transmissions used to deliver a packet over multiple hops to a destination. Distance vector routing is another more traditional cost metric that would be used involving hop count. Hop count is perfectly sufficient in highly reliable links with infrequent retransmissions to capture the cost of packet delivery. This does not suit the wireless sensor network environment with links of

varying quality and stringent constraints on power. There are times when a longer path requiring fewer retransmissions would be better than a shorter path requiring more retransmissions. An example of this would be if it would be far more efficient to transmit a packet over a given distance with multiple hops than to transmit the same packet over that distance with a single hop. [52]

Motes broadcast periodic beacon messages to all other motes within their radio range for initial formation of the multi-hop network. Figure 10 depicts a wireless sensor network in which only nodes one and two are inside the radio range of node zero, the BS, while nodes one, two, three and four are within radio range of each other. It also demonstrates a potential transmission path from node three to the BS. Health packets are periodically transmitted to the BS along with other data packets. Health packets contain information pertaining to mote performance within the mesh network with specific regard to radio traffic. Other information such as battery voltage and the parent's Received Signal Strength Indicator (RSSI) data is also included. [52]

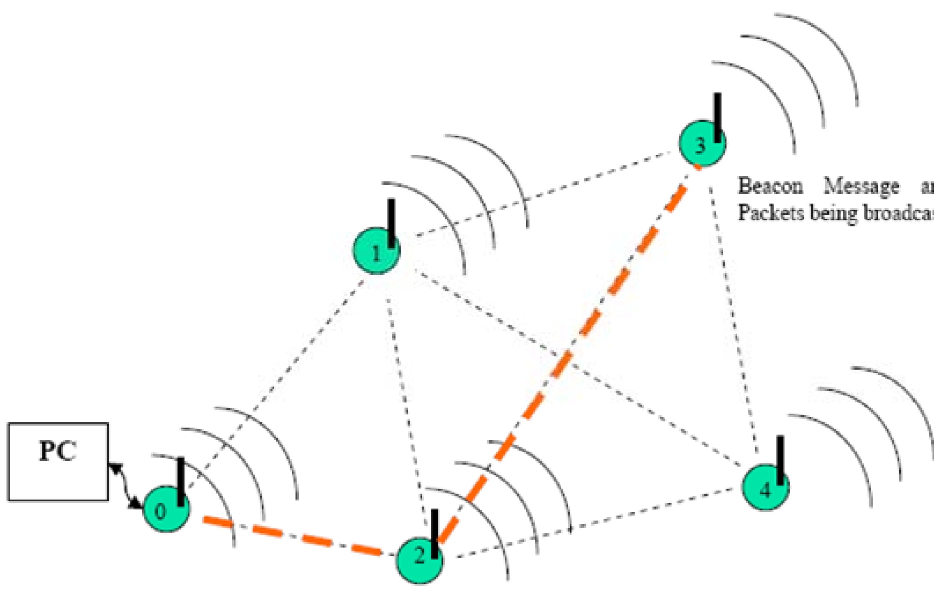

Figure 10. Broadcasting Beacon Messages and Health Packets (After Ref [52])

Beacon messages contain information that indicates to other motes the energy required to transmit a message to the BS. This is the cost value which has a higher cost when more energy is required to complete the transmission. The cost metric is used to minimize the total amount of energy that is consumed in transmitting information to the BS mote. The estimated cost value of each node in the mesh network is broadcast periodically in a beacon message. This message also includes the number of hops required for a message to reach the BS mote as well as a packet sequence number and a Neighborhood List (NL). The packet sequence number from a given mote is a sixteen bit integer that is incremented every time that mote transmits a message. The information contained on the NL pertains to all of the motes within the reception range of the mote in question. There are two parts to the information on the NL: the identifier of the Neighborhood Mote (NM) and an estimate from that mote of its ability to hear its neighboring motes. The value of this estimate is attained by monitoring the sequence numbers of the messages received from the NM. A computation of the percentage of lost packets can then be performed in order to determine the quality of the link between the nodes. [52]

The quality of the link between motes in both directions is important. Losing an acknowledgement for a packet that has already been received would lead to a retransmission that wastes as much energy as if the packet were actually lost. The MT cost for each link is estimated by calculating the product of the inverse of the forward direction, sender to receiver, link quality and the inverse of the backward direction, receiver to sender, link quality. The MT cost otherwise referred to as the link's cost to its parent can be written as in Equation (1) below.

$$MT_{ToParent} = \frac{1}{LinkQuality_{forward}} \times \frac{1}{LinkQuality_{backward}} = \frac{1}{SendQuality} \times \frac{1}{ReceiveQuality} \quad (1)$$

As a simple numerical example, assume the *SendQuality* between a node and its parent is 25% (0.25) and the *ReceiveQuality* is 20% (0.20), the MT cost of the link between the node and its parent would be 20. The MT cost of the parent to the BS would be the total cost of all hops to the BS as in Equation (2) below.

$$\text{Parent's cost} = \sum(MT) \quad (2)$$

It then follows that the total MT cost of the node to the BS can be calculated as in Equation 3.3 below.

$$\text{Node cost} = \text{Parent's cost} + \text{Link cost to Parent} = \left[\sum(MT)\right] + MT_{ToParent} \quad (3)$$

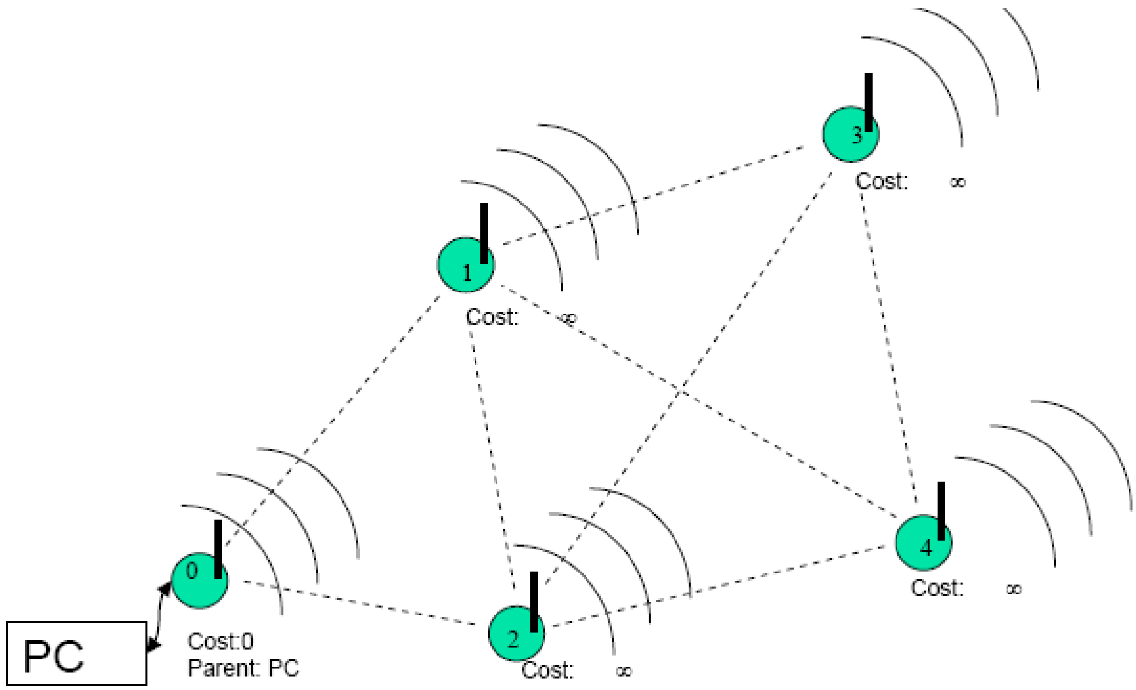

Figure 11. Network Status during Initial Configuration (After Ref [52])

Figure 11 depicts the status of the network in the initial stage of configuring itself. The beacon message from the BS has a MT cost to the PC equal to zero and all other motes have an MT cost of infinity because they have not established any message routes back to the BS. Since parent selection has not been completed the beacon messages contain no routing entries. Therefore, when a mote sends out any data messages they are sent with a broadcast address. Eventually, all of the motes within the receiving range of the BS will have received beacon messages from the BS. Messages can then be forwarded to the BS from these motes. The messages that the BS receives from these motes are then included in its NL for its broadcasting beacon messages. The motes within

receiving range of the BS will in turn include the BS and other neighboring motes in their NL's for their beacon message broadcasts and parent selection can commence. Once parent selection is complete, data message addresses change from a broadcast address to the parent's address. Mesh network formation propagates continues from this point to the motes that are outside the BS's transmission range and have not heard its beacon messages. Figure 12 depicts the status of the network once all of the MT cost values have been established and illustrates the most efficient path from node three to the BS, node zero, is not necessarily the one that is the shortest. [52]

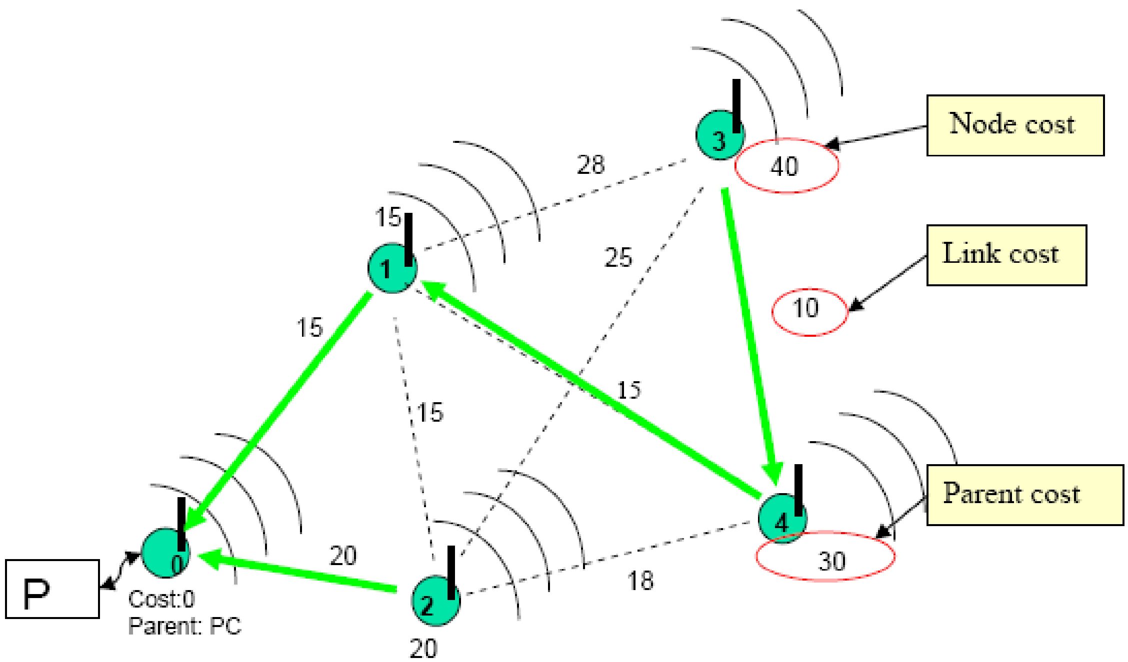

Figure 12. Network Status with Cost Values (After Ref [52])

3. XMESH PACKET FORMAT

Figure 13 depicts the TinyOS message structure. It consists of a five byte header, a twenty-nine byte payload and a two byte Cyclic Redundancy Check (CRC). The CRC is used to determine if the packet was received successfully. The TinyOS message header consists of the following fields: a two byte address, one byte for the active message type,

a one byte group identifier, and one byte for the payload length. The active message type field identifies whether the message being sent is data, routing or broadcast. Since payload size is variable the payload length field represents the amount of actual data that is present in the payload. [52]

Header (5)	Payload (29)	CRC (2)

Figure 13. TinyOS Message Structure (From Ref [54])

Figure 14 depicts the TinyOS message packet transmission sequence. Before listening for an idle channel prior to message transmission a simple Carrier Sense Multiple Access based (CSMA-based) MAC is employed to generate a random delay. After this delay if the channel is discovered to be busy, it waits and again generates a random delay over a predetermined window. Subsequently, when the channel is clear the transmitter is activated and the motes in the network are synchronized by sending the preamble and frame synchronization bytes. There are three types of preamble: the standard preamble, the short extended preamble, and the full extended preamble. The Standard Preamble is used to route data traveling on the last hop to the BS. Since the BS has significantly higher traffic than the rest of the network, the use of the standard preamble packet reduces the power consumption required of the nodes surrounding the BS. The short extended preamble is used for all traffic being routed by a node that it does not originate itself. All data that is only being forwarded by a node is transmitted with the short extended messages except for those messages traveling directly to the BS which use the standard preamble packet previously discussed. The full extended preamble is used for nodes to transmit data messages that they locally generate. It is also used for link monitoring and routing discovery. Transmission of route update messages uses the extended preamble message for the discovery of new links and so that the nodes can become synchronized into the network. The transmitter is turned off once message transmission over the Small Computer System Interface (SCSI) Parallel Interface (SPI)

port is complete. This triggers the event which signals to the application that the transmission has been completed. The TinyOS packet is assembled at the receiving mote and the CRC and the group identifier are checked. The packet is rejected if the CRC or the group identifier does not match anticipated values. If the CRC and the group identifier are appropriate, the packet is accepted and the application signals that a packet has been received. [52]

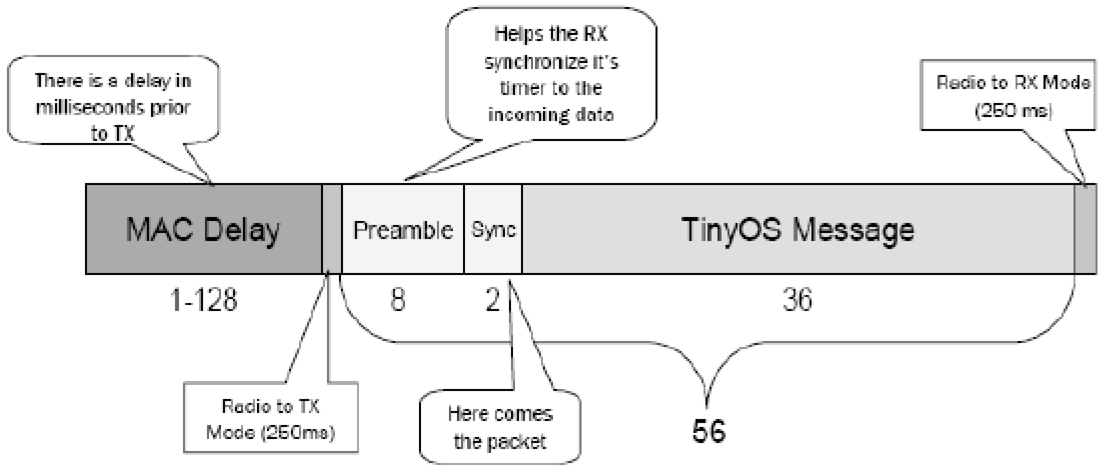

Figure 14. TinyOS Message Packet Transmission Sequence (From Ref [54])

E. SUMMARY

The purpose of this chapter was to discuss topics related to wireless sensor networks and their constituent components that were used for the experiments performed as part of this thesis. The specific components of the network produced by Crossbow Technologies were discussed. Then an overview of the operating system, TinyOS, was provided. Finally, a description of the routing protocol, XMesh, was presented.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENTAL STUDY

A. CHAPTER OVERVIEW

This chapter discusses the experiments undertaken and the results that they produced. The experiments were performed under a variety of conditions with several parameters of interest. Mote performance in the areas of radio reception range, signal quality, network stability, and network formation times were evaluated with respect to different surfaces and orientations at different proximities. After some baseline results were obtained for motes on an arbitrary hard surface, they were tested on the surface of the water and floating below the water's surface without being completely submerged. Submerged performance was not specifically evaluated, but is discussed briefly. Performance metrics were then evaluated from the data gathered during these experiments.

B. EXPERIMENTAL PROCEDURE

All experiments were performed using MICA2 motes manufactured by Crossbow Technologies utilizing the high transmit power level of +5 dBm, which is 1.64 mW. The specific data gathered for each of the following sections was gathered for a variety of different situational conditions. In order to gather a baseline of dry performance data, mote performance was evaluated on a hard solid surface with little possibility for multi-path reception. A tennis court was chosen as these conditions most closely approach those of the open watery surface used for the remainder of the experiments. A number of other dry implementation scenarios were evaluated in the study by Mark E. Tingle in March 2005. The communication and sensor ranges of the MICA2 mote at a fixed radio transmission power over four types of terrain were tested. The four terrain types were open terrain, outdoor wooded terrain, urban outdoor terrain and indoor terrain, none of which were optimally suited for comparison to water in this context. Next, motes were tested floating completely on the surface of the water. Following this, tests were completed with one mote floating completely on the surface of the water with the others

floating just below the surface of the water without being completely submerged. Maintaining an area above the mote open to the air was the critical element of this and the following segment of testing to prevent the futility of trying to actually transmit through the water, which will be discussed later. Finally, tests were performed with all motes floating just below the water's surface. Figure 16 depicts the difference between floating on the water and floating in the water. The easiest way to achieve neutral buoyancy was to be able to control the volume of the container. This was accomplished using zip-lock sandwich bags. The bags were inflated slightly to provide positive buoyancy and weighted down with two rolls of fifty pennies each along with the mote until neutrality was achieved. Floating on the water the bags were completely inflated with no additional weighting added. [5]

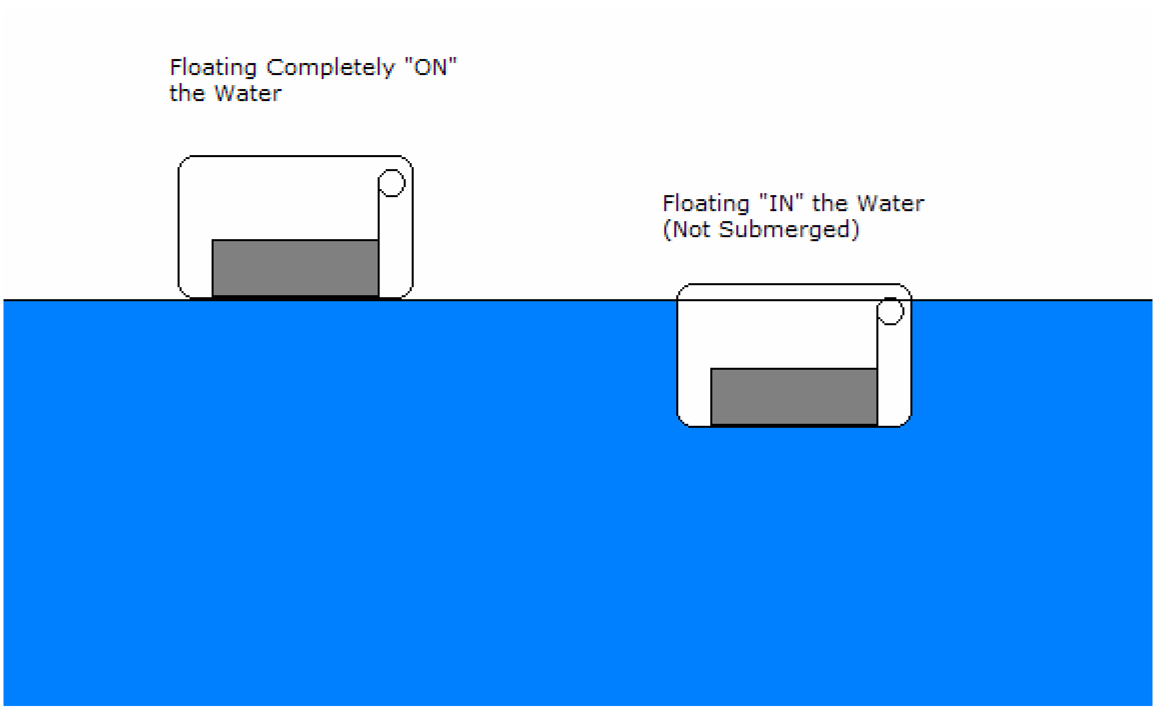

Figure 15. Mote Placement "ON" versus "IN" the Water

Based on the study by Swee Jin Koh in March 2006 which provided a detailed study of the performance of mote antennas and their radiation characteristics, a consistent

antenna orientation was used. Mote antennas were oriented perpendicular to the sensor ground plane and parallel to each other. This matches up the respective polarizations and represents the case with minimal losses. Figure 16 depicts the antenna orientation. [7]

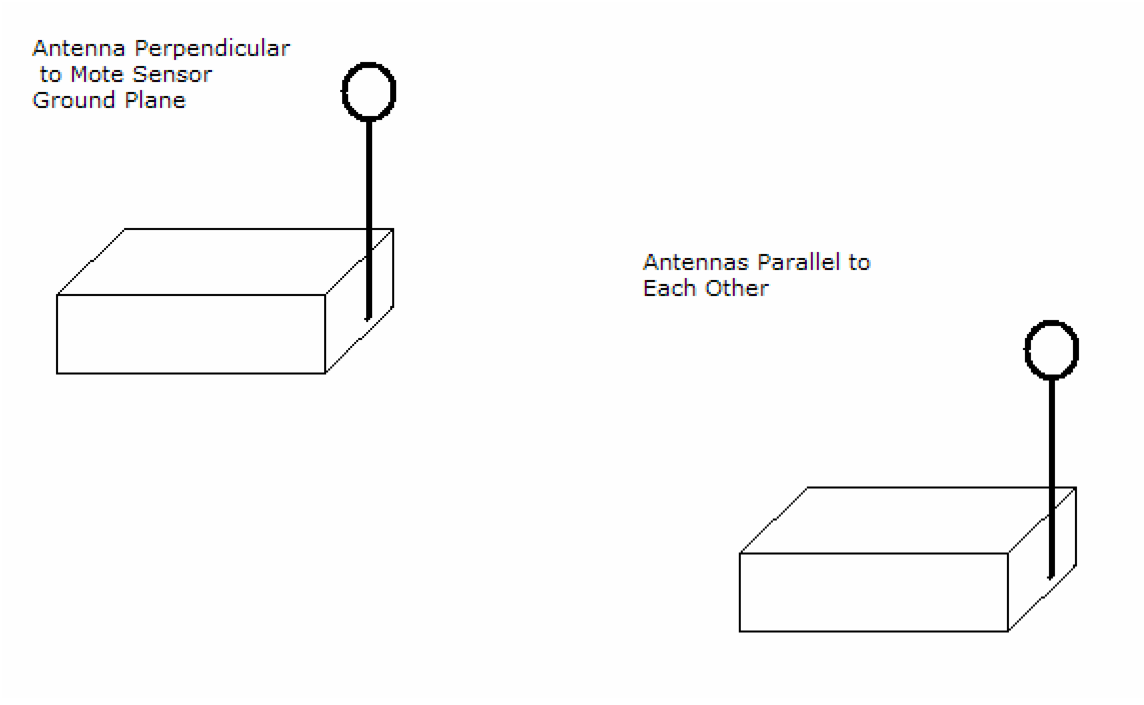

Figure 16. Mote Antenna Orientation

1. Radio Range

Radio reception ranges between communicating motes was determined using a simple procedure involving Mote View software while utilizing three motes. The first mote, node zero, was established as the gateway or base station. The second mote, node one was placed such that node zero, the base station, became its parent. The final mote, node two, was positioned to establish node one as its parent. This configuration was established due to difficulties involved in attempting to float the base station and its associated connections to the PC in the water while maintaining the appropriate antenna orientation. At times it was noted that node two's parent would switch to node zero, but

only at shorter ranges which had no real bearing on the range testing. Once confirmation of network communication between the nodes was verified, the motes were moved apart incrementally until the link was lost. Node two was then moved back toward node one until the link was reestablished. This process was repeated no less than four times to ensure consistent results.

2. Link Quality

Link quality was also measured using Mote View software. Link quality is defined as the ratio of the number of information packets received to the total number of information packets actually sent. This value was calculated from data provided by Mote View. Mote View provides retransmission data in the form of "retries" expressed as a percentage. This represents the percentage of the time that a node had to retransmit a packet due to the lack of a link-level acknowledgement. In order to determine link quality from this quantity one hundred percent was added to the percentage of retries and that result was divided by one hundred and reciprocated. This is shown in Equation (4) and gives the fraction of sent packets that were received and acknowledged.

$$LinkQuality = \frac{1}{\left[{}^{(100\% + \mathrm{Re}\,try\%)}\!\big/_{100}\right]} \tag{4}$$

As an example, if the retry value was 6.5, this means that 6.5% of the time a packet is retransmitted due to the lack of a link-level acknowledgement. Therefore, adding the extra 6.5% that were retransmitted to the 100% that were received and acknowledged results in a ratio of the total number of information packets sent to the number of information packets that were received. This is the inverse of the desired valued for link quality and reciprocating it will result in the link quality. Reciprocating the fractional representation 106.5%, which is 1.065, results in a fractional value of 0.939, which would be link quality of 93.9%. Link quality was measured incrementally during the determination of radio reception ranges at all ranges noted. [55]

3. Network Formation

Network formation was timed from the initiation of the network with motes at various ranges. The network was considered to be initiated for this portion of the experiment when the motes were activated and moved into position as quickly as possible. This was done to simulate a mass dispersion of motes into an inaccessible area where the motes would be activated en masse and inserted to perform their function. In this instance, activated means that power was applied to the motes or that they were switched on. The network was considered formed and time stopped when all of the nodes set in place and activated were accounted for by the base station with their data being received. This part of the experiment was performed with nine motes, including the base station, situated in a relatively uniform distribution that would allow great flexibility in parent selection. The nodes of the network were configured into rows that layered away from the base station with three in the first row, two in the second, and three in the last. The base station is node zero with all of the other nodes being one through eight as they get further away. Figure 17 depicts the formation and gives an example of the parents selected. The procedure was performed at three ranges for each situational condition except the both “IN” the water situation. The first range is one meter, one half meter for the both “IN” situation, well within the most reliable region. The next was at the far edge of the reliable region, one meter for the both “IN” situation. The last was at the maximum radio reception range as a representative case for the transition region. The procedure was repeated four times at each range.

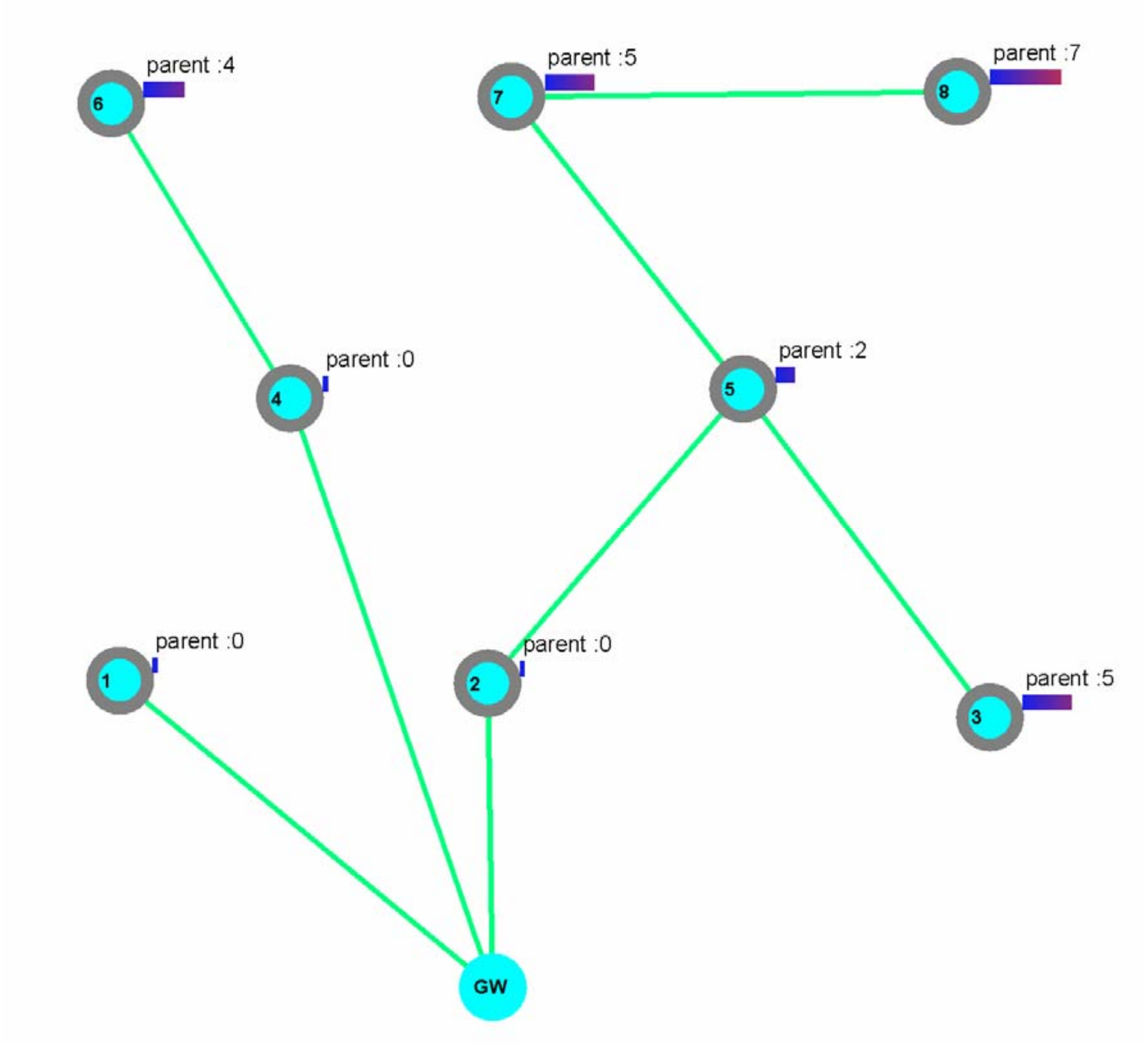

Figure 17. Node Formation and Parent Selection

4. Network Stability

Network stability was determined by observing the number of times that a node underwent a change of parent. During network formation and once the network was established at each given range, each node was monitored for parent changes over a period of not less than thirty minutes and the values noted. This scenario does include one example of network response to a node being lost. During one of the experimental trials a mote sank to the bottom of the lake where the experiments took place. The same mote

configuration was used for these experiments as described in the previous section and Figure 18 depicts an alternate parent selection for the same node formation shown in Figure 17. This procedure was also repeated four times.

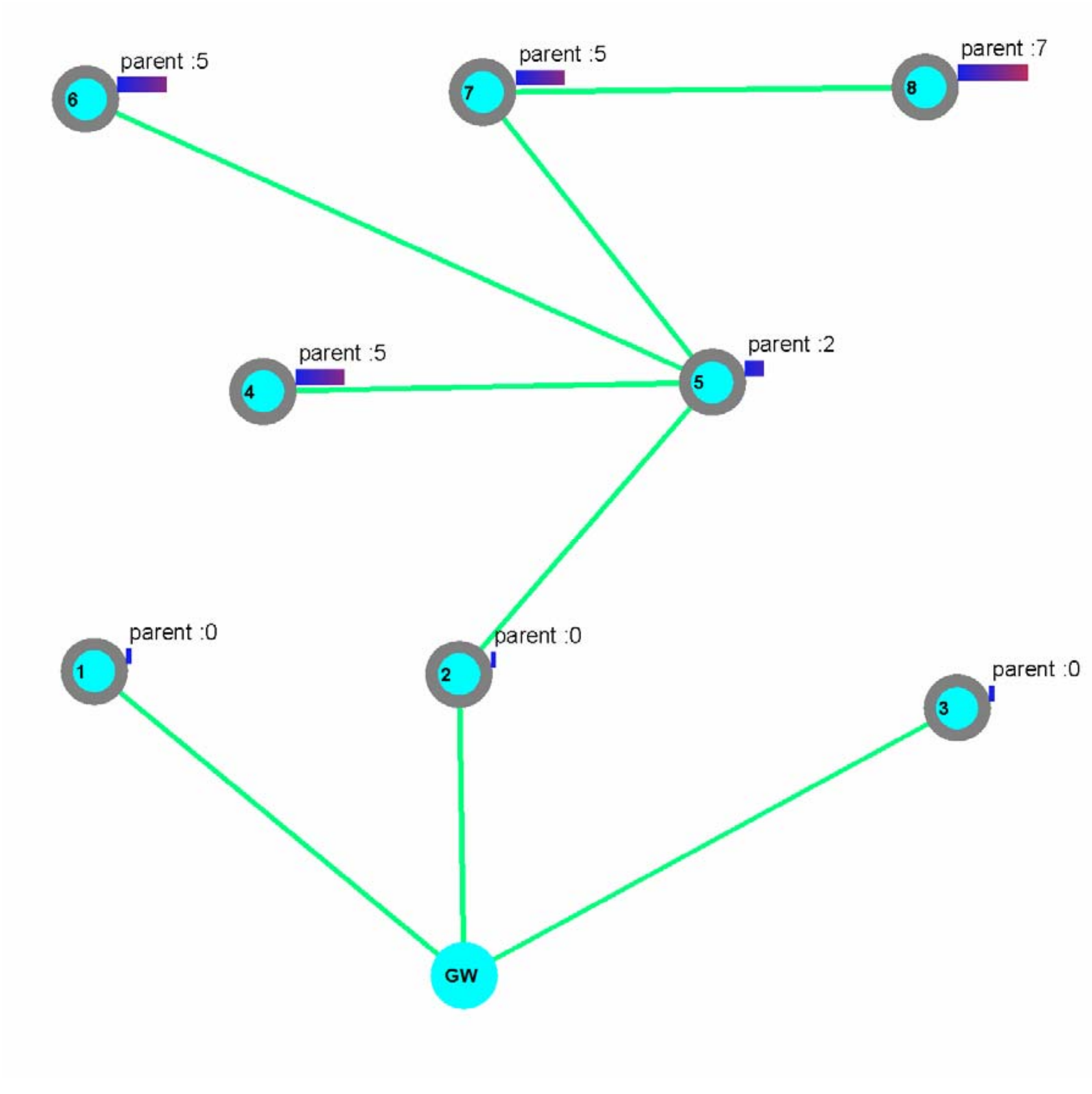

Figure 18. Alternate Parent Selection for Node Formation

C. EXPERIMENTAL RESULTS

1. Radio Range

Propagated ground waves take three separate paths to the receiver, the direct wave, the ground-reflected wave, and the surface wave. A ground wave's field strength depends on a number of factors. These factors include the radio frequency, transmitter power, transmitting and receiving antenna characteristics, including polarization and height, electrical characteristics of the terrain, and electrical noise at the receiver site. All of these factors remained constant for the purposes of these experiments save one, the electrical characteristics of the terrain. Specifically, these are the conductivity and dielectric constants of the terrain. The direct path component of the ground-wave travels from the transmitting antenna to the receiving antenna directly, while the ground-reflected path is reflected off the ground or sea en route to the receiving antenna. Once reflected off of the terrain's surface, the phase of the ground reflected wave can shift up to 180 degrees as the grazing angle approaches zero. The ground-reflected path also travels a longer distance in reaching its destination also adding to the overall phase shift. The results of this phase shift can be constructive or destructive. Both the transmitting and receiving antennas on or very near the surface presents a worst case destructive scenario with a near 180 degree phase shift. Ignoring any surface wave component, the net result in this case is a weakening of the direct wave that is roughly equal to the strength of the reflected wave resulting in a near zero signal amplitude. The surface wave component of the ground-wave is affected primarily by the frequency, conductivity and dielectric constant of the terrain. When both the transmitting antenna and the receiving antenna are close to the ground, the direct wave and ground-reflected wave tend to cancel each other. The surface wave is guided by the earth's surface, but extends up to considerable heights. Diminishing in strength with increased height its intensity becomes negligible at about one wavelength above the ground and five to ten wavelengths above sea water. The ground absorbs part of the surface wave's energy attenuating the electric intensity of the surface wave. This attenuation is dependent on the conductivity of the

terrain over which the wave travels. Sea water is a good surface for surface-wave transmission due to its high conductivity. [56]

a. Hard Surface

In continuing a portion of the research conducted by Mark Tingle in his March 2005 study some expectations were made based on his results. During his research he observed radio reception ranges did not exceed four meters with motes on the ground in open outdoor terrain that consisted of a grassy field with little opportunity for multi-path reception. Moving the experiment to a hard solid surface with more favorable conductivity and dielectric characteristics, still little opportunity for multi-path reception and motes on the ground produced radio ranges out to seven meters. Motes were moved incrementally one meter at a time beginning at one meter. When moved beyond seven meters to eight meters reception was lost and regained when returned to seven meters. An increase in radio range was expected, but the magnitude of the change being 75% demonstrates the significance of terrain with respect to mote performance. These results were consistent over four repetitions of this cycle and are graphically depicted in Figure 20 which follows in the section covering link quality. [5, 56]

b. On Water Surface

While sea water possesses the best conductivity and dielectric characteristics for surface wave propagation, a fresh water lake was used for the purposes of these experiments. Even so, moving the experiment from a hard solid surface to fresh water with even more favorable conductivity and dielectric characteristics, little opportunity for multi-path reception, and motes on the surface of the terrain produced radio ranges out to nine meters. Again motes were moved incrementally one meter at a time beginning at one meter. When moved beyond nine meters to ten meters reception was lost and regained when returned to nine meters. While the 29% increase in radio range is not as dramatic as the increase from the previous section, it is nevertheless significant and further demonstrates the importance of the terrain and its effects on mote

performance. These results were consistent over four repetitions of this cycle and are graphically depicted in Figure 19 which also follows in the section covering link quality. [56]

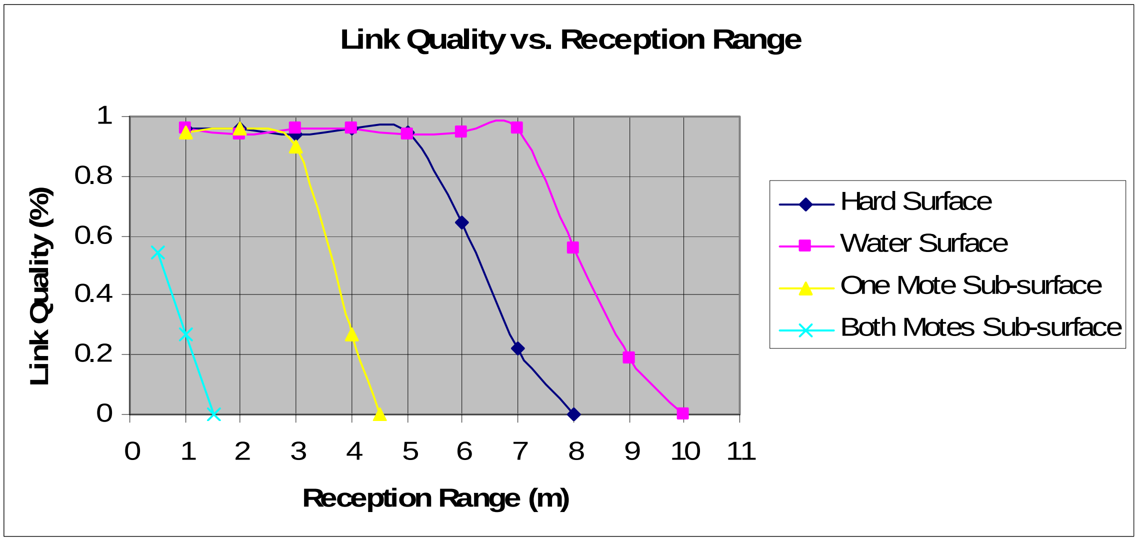

Figure 19. Link Quality versus Radio Reception Range

c. Submerged

Water is a poor medium for the propagation of RF signals. In anything besides free space an RF signal becomes compressed, slows down, and is attenuated more rapidly. This is especially true in salt water. The experiments documented here were performed using fresh water which, while not having as great an effect on signal losses as salt water, still causes severely detrimental signal losses. Figure 20 depicts the effects of fresh water and salt water as compared to free space on signals of various frequencies. The x-axis represents the distance that the signal must travel in mm. The y-axis represents the losses experienced by the signal over that distance in dB. The lines show losses in free space (blue), fresh water (green), and salt water (red). These losses are also shown for various frequencies beginning with the topmost line in each color at 100 MHz and progressing to the bottom most line in each color at 10 GHz with lines at 1

MHz and 5 MHz respectively. The 10 GHz line is not shown for sea water as it is out of range on this scale. The submerged radio reception range between two communicating motes was on the order of centimeters for which no foreseeable purpose can be determined. No further experimentation under these conditions was performed. [57]

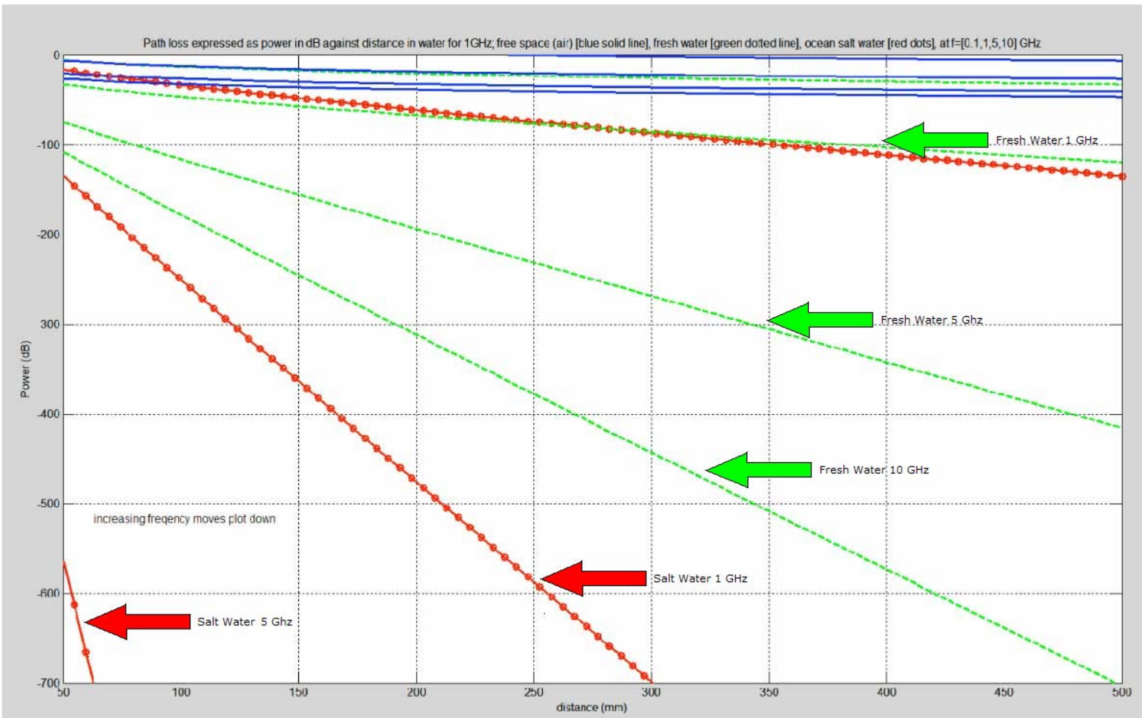

Figure 20. Path Loss Power versus Distance in Free Space (blue), Fresh Water (green), and Sea Water (red). Frequencies Increase from Top to Bottom, 0.1, 1, 5, and 10 GHz respectively. (From Ref. [57].)

d. Below Water Surface

This portion of the experiment took place in two stages demonstrating more of the detrimental aspects of water as part of the communication environment. In the first stage, data was collected with one of the nodes “ON” the water, completely above the surface of the water as before while the other node was “IN” the water, floating completely below the surface, but not completely submerged, as discussed above. In the second stage, data was collected with both of the nodes “IN” the water, floating just

below the surface. With this geometry the advantages provided by water with respect to surface wave propagation are never fully realized. The water between the motes acts as a barrier until the signal radiates clear of it. At this point only a portion of the signal, which is weaker in magnitude, is allowed to propagate along the surface. [7, 56]

(1) One Node "IN" the Water/One Node "ON" the Water. Once placed in this configuration, motes were moved incrementally one meter at a time beginning at one meter. When moved beyond four meters to five meters reception was lost and regained when returned to four meters. With the shorter range the mote was then moved away only another half meter when again the link was broken. This decrease of just over 55% from the open water trial is very significant. It begins to delineate the serious shortcomings involved with using this technology with respect to water. These results were consistent over four repetitions of this cycle and are graphically depicted in Figure 21 which follows in the section covering link quality.

(2) Both Nodes "IN" Water. In this final configuration, motes were again moved incrementally beginning at one meter, but this time only one half meter at a time. When moved beyond one meter to one and a half meters reception was lost and regained when returned to one meter. This result, with another 75% decrease in radio range from the previous case, clearly demonstrates that compelling issues remain for these systems in this environment. These results were consistent over four repetitions of this cycle and are graphically depicted in Figure 21 which follows in the section covering link quality.

2. Link Quality

The data measured for link quality was recorded incrementally in conjunction with the radio reception range data. The retransmission percentage was averaged over a five minute period at each range increment and used to calculate the corresponding link quality as previously described in the procedure section. Figure 21 depicts the qualities of the links at the various ranges. This figure clearly demonstrates three distinct performance regions for each situation except the last which only shows two. The first three trials have distinct regions where the performance is very reliable, averaging in the

middle to high nineties for link quality expressed as a percentage. This region for the hard surface, water surface, and one “ON”/one “IN” trials extends out to ranges of five meters, seven meters, and three meters respectively. The trial with both motes “IN” the water exhibited no such region as link quality improved only marginally inside of one half meter where the chart stops. All trials displayed attributes that fall into a transitional region where reception was possible, but link quality was not as high. This region for the hard surface, water surface, one “ON”/one “IN”, and both “IN” trials extends from the reliable region, except in the case of the both “IN” trial, out to the maximum radio range of seven meters, nine meters, four meters, and one meter respectively. Beyond this maximum radio reception range is the unusable region beyond which no communication is possible. This behavior was predictable and similar from case to case.

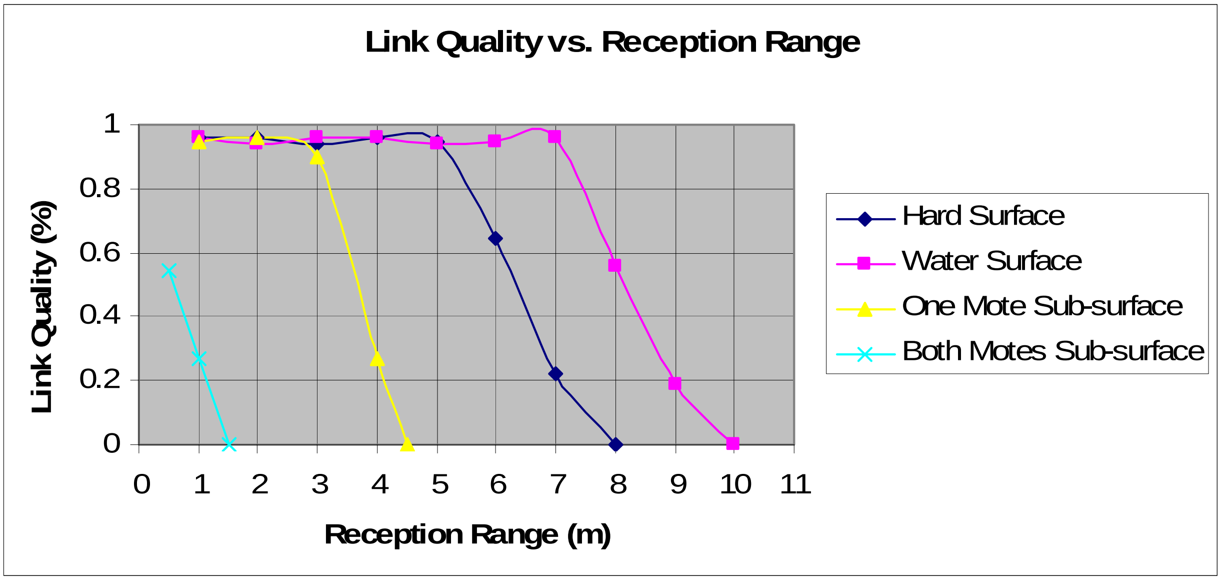

Figure 21. Link Quality versus Radio Reception Range

3. Network Formation

Network formation times were recorded as described in the procedure section and were equally as predictable and similar across all cases. With motes operating anywhere in their respective reliable regions as discussed in the previous section, network

formation was completed in one to two minutes. With motes operating at maximum radio reception range, as a representative case for the transition region, network formation was completed on average in four to five minutes. This demonstrates the importance of reliable communications in even this aspect of the network and was the case for all situations except for the both “IN” the water scenario which were on average a full minute longer than all of the other situations. This geometry poses significant problems for mote to operate in. Figure 22 depicts the specific results of the hard surface and both “ON” the water network formation times while Figure 23 depicts the one “ON”/one “IN” the water and both “IN” the water network formation times. These results made sense as they paralleled the overall communications difficulties demonstrated by the link quality measurements discussed in the previous section. Four trials were conducted at each of the three ranges described in the procedure section for all situations except the both “IN” case. For all situations except the both “IN” case the ranges were one meter, the maximum reliable range, and the maximum reception range at the edge of the transition region. For the both “IN” case the trials were conducted at one half meter and one meter.

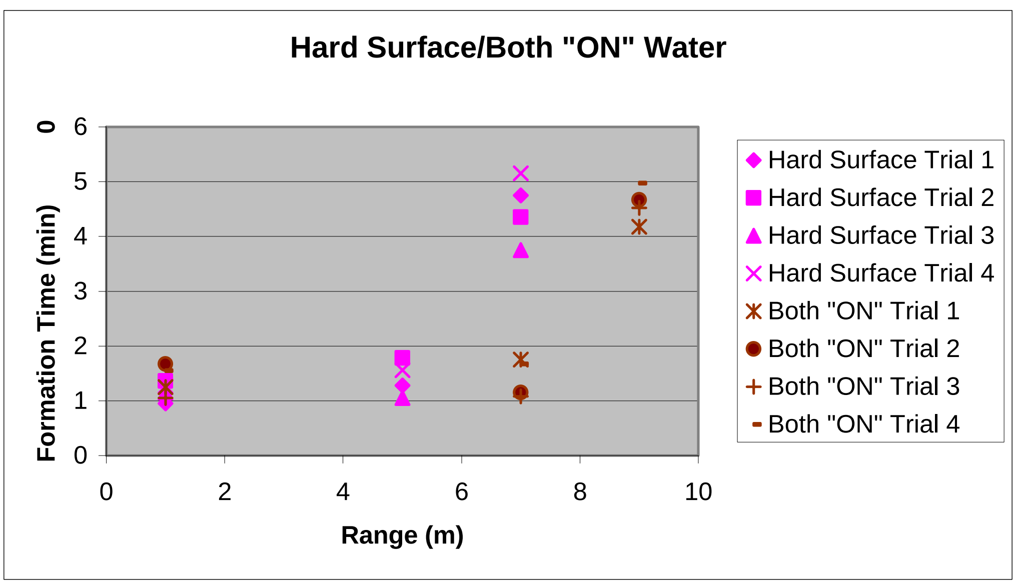

Figure 22. Hard Surface and Both “ON” Water Network Formation Times

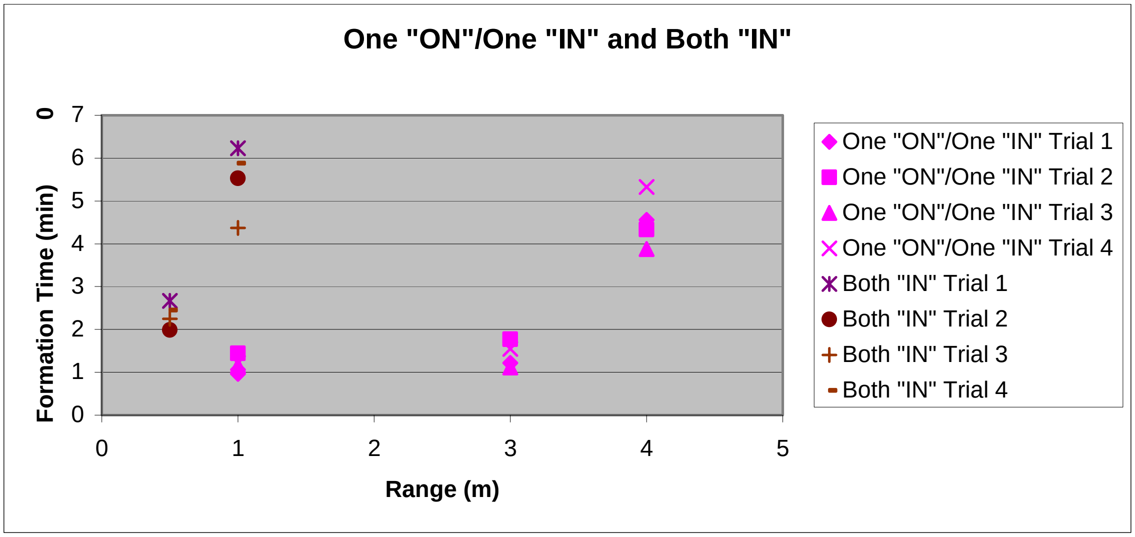

Figure 23. One “ON”/One “IN” and Both “IN” Water Network Formation Times

4. Network Stability

Network stability was evaluated as described in the procedure section and was similar across all cases except the both “IN” cases. The hard surface and both “ON” the water cases were nearly identical. The one “ON”/one “IN” case had one minor difference from these cases due to its configuration. In the one “ON”/one “IN” case the base station is “ON” the water with the closest row of three motes “IN” the water. The next layer of two motes was also “ON” the water with the last row “IN” the water. This formation is depicted in Figure 24 and produced an interesting result. The both “IN” case further demonstrated the difficulties associated with this geometry with its results standing apart from the other situational trials completely.

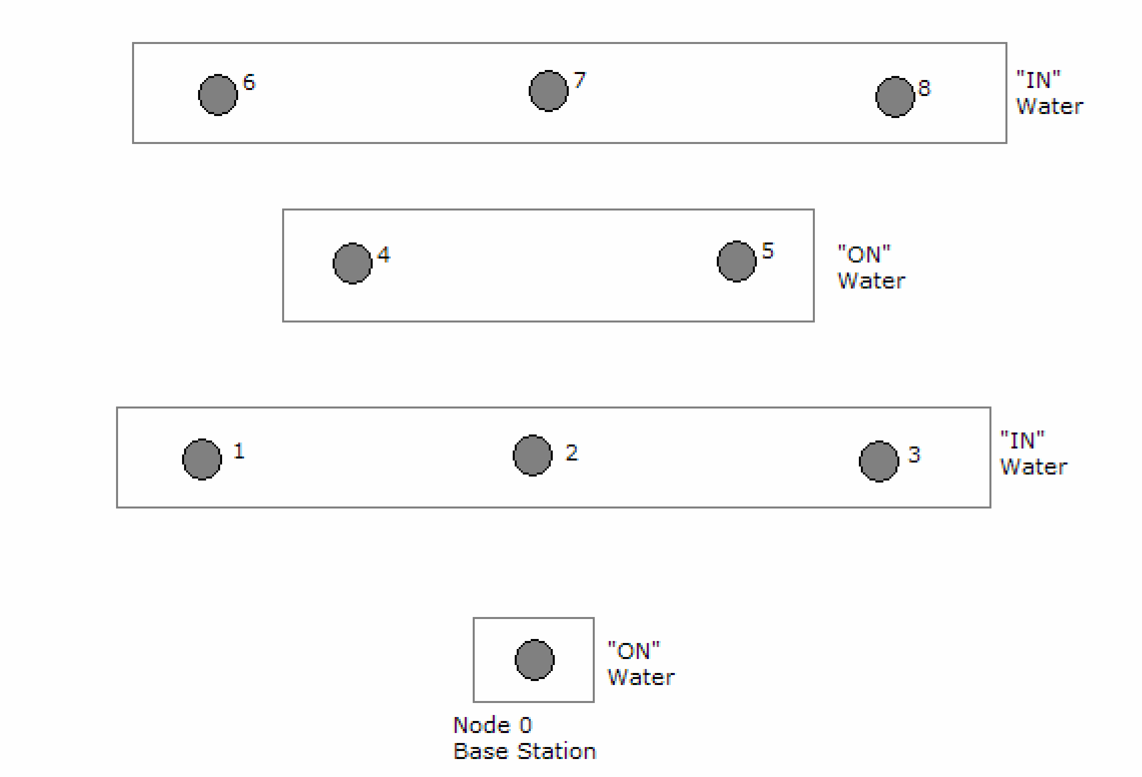

Figure 24. Network Stability Testing One “ON/One “IN”

Through all of the experiments the network exhibited great stability once network formation was complete. Most parent changes occurred during network formation. While operating within their respective reliable regions established in the radio range section, each node underwent a parent change on average just over once in a thirty minute period. While operating at maximum radio reception range, again as a representative case for the transition region, each node underwent a parent change on average less than three times in a thirty minute period. On only a couple of occasions did a node change parents a maximum observed five times in the thirty minute period while in the reliable range. These could be attributed in part to the mobility of the network during the cases in which the motes were in the water as they drifted in place. The lone exception to this was the both “IN” the water situation which has no reliable region. On the lone occasion that a node was lost, all routing was redirected and the network reorganized in less than one minute. Figure 25 depicts the results from the hard surface situation while Figure 26

depicts the results from the both “ON” the water situation. These figures show the number of parent changes that occurred for each node in each of the trials at the ranges described in a thirty minute period. The results of the hard surface were nearly identical.

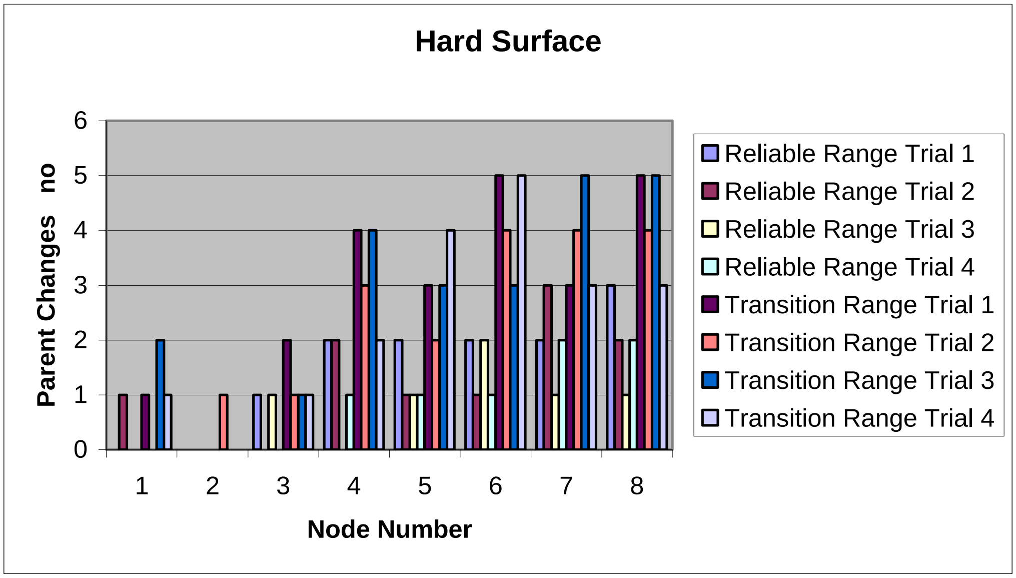

Figure 25. Hard Surface Network Stability Trials Parent Switching

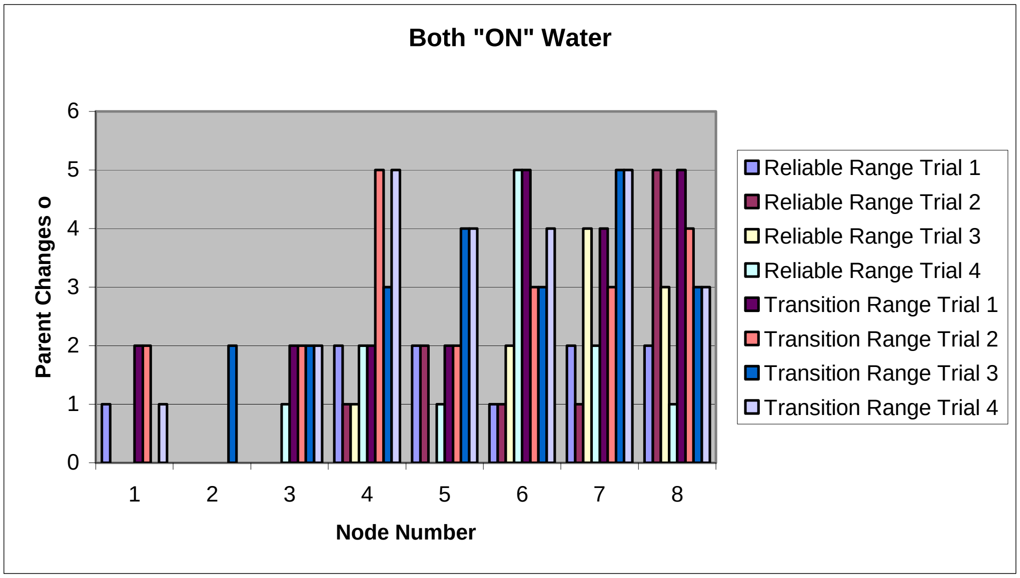

Figure 26. Both "ON" the Water Network Stability Trials Parent Switching

a. One "ON"/One "IN" Network Stability Trial

In all of the other trial cases, the nodes closest to the base station established and maintained the most stable links directly with the base station with the fewest number of parent changes, if any parent changes were made at all. This is depicted in Figures 25 and 26. However, in this trial the other nodes that were "ON" the water established and maintained the most stable links. This is due to the geometry of the links that were involved in order to even make this trial possible. With the ranges set in order to allow one "ON"/one "IN" links to be established, all motes that were "ON" the water were well within the reliable ranges established for both being "ON" the water. It came as no surprise then that nodes four and five in the second row away from the base station established and maintained the most stable and reliable links directly with the base station. There is a greater than 500% increase in parent changes between the closest nodes and the rest of the nodes in general. Figure 27 depicts these results. Again this figure shows the number of parent changes that occurred for each node in each of the trials at the ranges described in a thirty minute period.

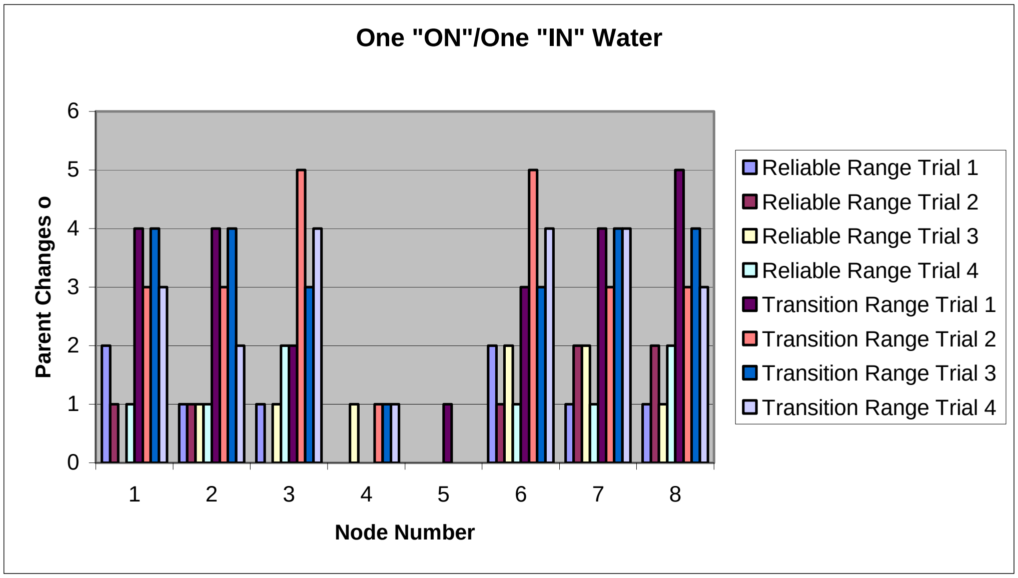

Figure 27. One “ON”/One “IN” Network Stability Trials Parent Switching

b. Both “IN” Network Stability Trial

This last case stood apart from the other trials in that all nodes demonstrated a higher degree of instability throughout its transition region including the three nodes closest to the base station. The nodes in general changed parents on average just fewer than three times, almost one full parent change more. A difference between the nodes closest to the base station and the rest of the nodes was noted, but to a lesser degree than in previous situations, only about a 33% increase in parent changes. Figure 28 depicts these results.

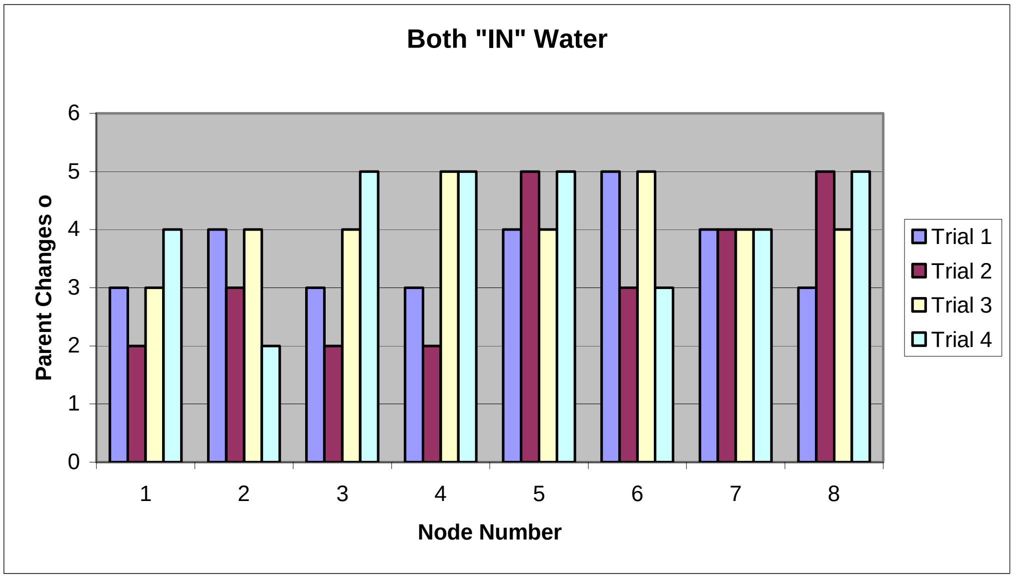

Figure 28. Both “IN” Network Stability Trials Parent Switching

As a final consolidation of data Figure 29 and Figure 30 are presented to demonstrate the effect of distance from the base station on overall network stability. Figure 29 depicts the overall data including the averages of all parent changes at the average distances from the base station for each trial. Figure 30 adds a contextual spin to the raw data by changing a few points to reveal a similarity that existed between all of the trials and cases. The first change made was to omit the point representing the nodes closest to the base station for the one “ON”/one “IN” situation. This represents the fact that the second layer of nodes in this case is the same as the closest layer of nodes in the other cases. Finally, for the cases with data points that did not lend themselves to forming straight lines already, the both “IN” case, the one “ON”/one “IN” cases, and the hard surface transition range case, the data points not associated with those closest to the base station were averaged. These produced lines with similar slopes that basically approximated what would be a graph representing parent changes versus the number of hops from the base station.

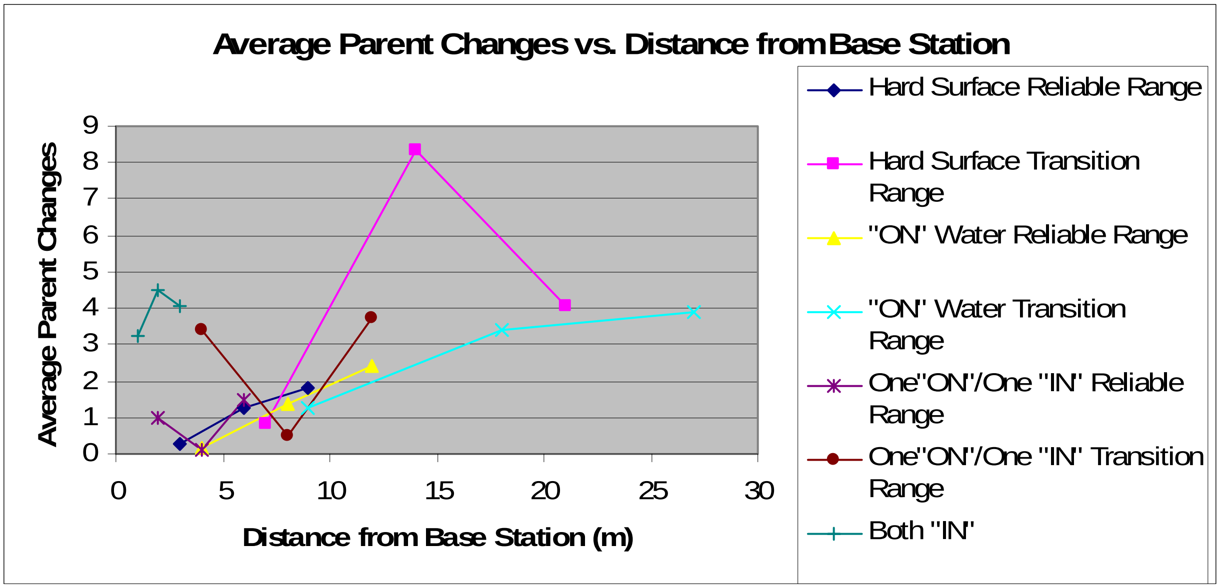

Figure 29. Average Parent Changes versus Actual Distance from the Base Station

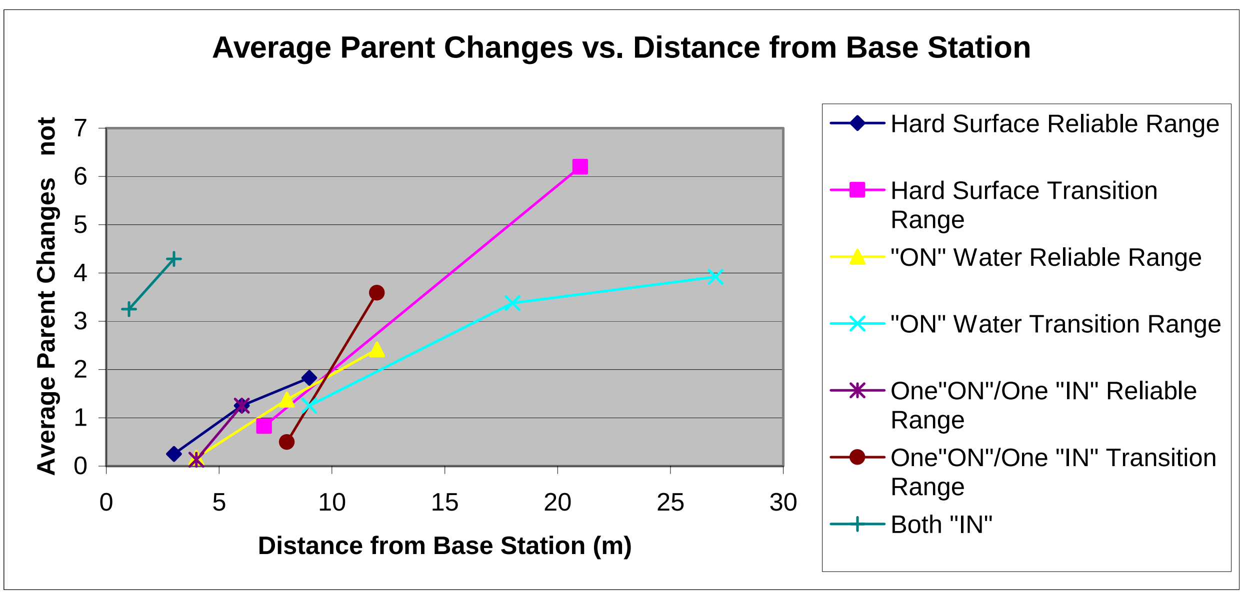

Figure 30. Average Parent Changes versus Average Distance from the Base Station

D. SUMMARY

The purpose of this chapter was to discuss the experiments undertaken as part of this thesis. It included a description of the procedures used for the gathering of all data as well as the various situations for which the data were gathered. Finally, the results of the experiments were presented along with a few observations as well as some of the ramifications.

V. CONCLUSIONS AND FUTURE WORK

With improvements in wireless communication and networking techniques coupled with the perpetually evolving technology of integrated circuitry, wireless, unattended sensor networks move ever closer to viable implementation. As motes continue to decrease in size while they conversely increase in capability, these systems become more science fact than science fiction for carrying out many of the already imagined tasks and provide new horizons from which to develop those as yet unimagined. Well within imagining at this time are performance metrics for existing technology in a variety of real world environments and scenarios. Previously, the environments were primarily land-based and dry. A background in submarines has resulted in the imagining of some of these same performance metrics in the water.

The objective of this thesis was to evaluate the performance of wireless, unattended sensor networks in a watery environment. The wireless, unattended sensor network used was produced by Crossbow Technologies. It utilizes the TinyOS operating system with the XMesh routing protocol. Two and eight sensor nodes with a base station node were used to form the architectures of the networks evaluated. Node communication ranges and link qualities were measured for a variety of conditions. Network formation times and stability with respect to parent changes were also noted under the same conditions.

A. CONCLUSIONS

The wireless, unattended sensor network performed admirably in situation where calm surface water conditions could be assured. With motes resting atop the surface of the water the performance even exceeded the dry land results. Surface path propagation over water allowed radio reception ranges out to a distance of nine meters whereas the radio range on a hard dry surface was only seven meters. However, this increase in range was undone by the very medium that provided it. A problem not as readily experienced on dry land, but very commonly associated with floating on the water is mobility. For the purposes of all of the experiments that took place in the water, a certain amount of

herding was necessary to keep the motes in positions appropriate for the gathering of data. The very nature of this type of network necessitates that the motes not be physically connected. The problem would lie in keeping the motes within range of each other. The flip side to this problem would be keeping them from clustering together as they follow whatever water flow is moving them. They could all end up gathered in the same place which defeats the point of a distributed sensor network.

Mobility notwithstanding, water precipitates other difficulties. Any water between two motes that are attempting to communicate greatly decreases their communication range to the point of futility. Completely submerged, motes have a communication range of a few centimeters and this system has no potential for practical use. The transmission geometries for situations where one mote is below the surface of the water reduce this capability by more than half to four meters. Twice as many motes would be required to cover the same area. With both below the surface of the water the communication range was reduced to one meter making the required sensor density too high for any serious consideration. Which of these situations even begins to reflect mote behavior in an ocean environment is unfathomable. With the potential for motes to be on opposite sides of a wave or temporarily submerged and constantly moving in a variety of directions additional research with more dynamic situations will be necessary.

B. FUTURE WORK

This thesis evaluated the performance of wireless, unattended sensor networks in maritime environments limited to calm fresh waters. The network consisted of MICA2 motes operating at 916 MHz on high power. The use of another type of mote at another operating frequency remains to be tested along with the possibility for any of the low power settings. Further research in this area could expand this topic to include the use of salt water. Seawater brings another aspect to the table with respect to surface wave propagation. A shallow evaporative duct exists over seawater up to heights of ten to fifteen meters which is known to effectively guide signals in the 3 – 20 GHz range. While motes do not currently operate in this range, it does present the possibility of using fewer higher power motes for this type of undertaking. Additionally, the effects of turbulent

water environments on these performance metrics could also be investigated. Finally, methods of dealing with the undesired aspect of water mobility could be looked into. The potential for new applications for this technology will most assuredly drive further research in a bevy of new directions.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] V. Clark, “Sea Power 21,” *Proceedings*, October 2002, http://www.navy.mil/navydata/cno/proceedings.html, last accessed March 2007.

[2] “Joint Vision 2020,” US Government Printing Office, June 2000, http://www.dtic.mil/jointvision/jvpub2.htm, last accessed March 2007.

[3] “Navy Concept Development and Experimentation Expeditionary Power Projection,” June 2001, http://www.dtic.mil/ndia/2001ewc/ncde.pdf, last accessed March 2007.

[4] C. Chong and S. Kumar, “Sensor Networks: Evolution, Opportunities, and Challenges,” *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, August 2003.

[5] Mark E. Tingle, “Performance Evaluation of Prototyped Wireless Ground Sensor Network,” Master’s Thesis, Naval Postgraduate School, Monterey, California, March 2005.

[6] Cheng Kiat Amos, Teo, “Performance Evaluation of a Routing Protocol in Wireless Sensor Networks,” Master’s Thesis, Naval Postgraduate School, Monterey, California, December 2005.

[7] Swee Jin Koh, **“**Study of RF characteristics of MICA2, the Sensor Networking System,” Master’s Thesis, Naval Postgraduate School, Monterey, California, December 2005.

[8] Ahmed I. Al-Shamma’a, Andrew Shaw, and Saher Saman, “Propagationof Electromagnetic Waves at MHz Frequencies Through Seawater,” *IEEE Transactions on Antennas and Propagation*, Vol. 52, No. 11, November 2004.

[9] Vitaly Bokser, Carl Oberg, Gaurav S. Sukhatme, and Aristides Requicha, “A Small Submarine Robot for Experiments in Underwater Sensor Networks,” *IFAC*, 2003.

[10] Karl, Holger, and Andreas Willig, *Protocols and Architectures for Wireless Sensor Networks*, pp. 15-357, John Wiley & Son Ltd, West Sussex, England, 2005.

[11] Stallings, William, *Data and Computer Communications*, Seventh Edition, pp. 9-38, Prentice Hall, Upper Saddle River, New Jersey, USA, 2004.

[12] J. Hill, R. Szewczyk. A. Woo, S. Hollar, D. Culler and K. Pister. “System Architecture Directions for Networked Sensors,” *Proceedings of Architectural Support for Programming Languages and Operating Systems*, pp. 93-104, Boston, Massachusetts, November 2000.

[13] “Mica The Commercialization of Microsensor Motes,” *Sensors*. April 2002. http://www.sensorsmag.com/articles/0402/40/, last accessed March 2007.

[14] K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, pp. 27-34, Prentice Hall, Upper Saddle River, New Jersey, 2002.

[15] C. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks Architectures and Protocols*, pp. 647-693, Prentice Hall, Upper Saddle River New Jersey, 2004.

[16] J. M. Rabaey, M. J. Ammer, J. L. Da Silva Jr., D. Patel, S Roundy, “Picoradio Supports Ad-hoc Ultra-Low Power Wireless Networking,” *IEEE Computer*, Vol. 33, Issue 7, pp. 42-48, July 2000.

[17] F.L. Lewis, *Smart Environments: Technologies, Protocols, and Applications*, Chapter 2, Edited By Diane Cook and Sajal Das, John Wiley, New York, 2004.

[18] Ding, Jin, Sivalingam K. Kashyapa, Lu Jian Chuan, “A multi-layered architecture and protocols for large-scale wireless sensor networks,” *Proceeding of Vehicular Technology Conference, 2003, VTC 2003-Fall*, 6-9 Oct. 2003, IEEE 58th, Volume 3, pp. 1443-1447.

[19] Younis, Ossama, and Sonia Fahmy “Distributed Clustering for Scalable, Long-Lived Sensor Networks,” *Proceeding of Ninth ACM MobiCom*, 2003, San Diego, California, USA,14-19 September 2003, pp. 1-2.

[20] J. Rabaey, M. Ammer, J. da Silva, D. Patel, and S. Roundy, “PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking,” *IEEE Computer*, vol. 33, no. 7, pp. 42-48, July 2000.

[21] G. Asada, M. Dong, T. Lin, F. Newberg, G. Pottie, and W. Kaiser, “Wireless Integrated Network Sensor: Low Power Systems on a Chip,” *Proceedings of Twenty-Fourth European Solid-State Circuits Conference*, pp. 9 – 16, 1998.

[22] E. Callaway, Jr., *Wireless Sensor Networks Architectures and Protocols*, pp. 21-44, Auerbach Publications, New York, 2004.

[23] T. Cooklev, *Wireless Communication Standards A Study of IEEE 802.11, 802.15 and 802.16*, pp. 35 – 218, IEEE Press, New York, 2004.

[24] C. Intanagonwiwat, R. Govindan and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,” *Proceedings of Association for Computer Machinery Mobile Computer Networking 2000*, pp. 56-67, August 2000.

[25] A. Perrig, R. Szewcyzk, V. Wen, D. E. Culler and J. D. Tygar, “SPINS: Security Protocols for Sensor Networks,” *Proceedings of Association for Computing Machinery Mobile Computing and Networking 2001*, pp. 189-199, July 2001.

[26] F. Ye, A. Chen, S. Lu, and L. Zhang, “A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks,” *Proceedings of IEEE International Conference on Computers Communications and Networks 2001*, pp. 304-309, October 2001.

[27] S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker, “GHT: A Geographic Hash Table for Data-Centric Storage,” *Proceedings of Association for Computing Machinery Workshop on Wireless Sensor Networks and Applications 2002*, pp. 78 -87, September 2002.

[28] W. Heinzelman, A. Chadrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks,” *Proceedings of Hawaii International Conference on System Sciences 2000*, pp. 4-7, January 2000.

[29] M. Horton, M. Turon, G. Baleri, and J. Hill, Notes for Wireless Sensor Network Seminar, Boston, Massachusetts, December 2004 (unpublished).

[30] A. S. Porret, T. Melly, D. Python, C. Enz, E. Vittoz, “Tradeoffs and Design of an Ultra Low Power UHF Transceiver Integrated in a Standard Digital CMOS Process,” *Proceedings of the 2000 International Symposium on Low power electronics and design*, pp. 273-278, Rapallo, Italy, 25-28 June 2000.

[31] K Sohrabi, et al., “Protocols for Self Organization of a Wireless Sensor Network,” *IEEE Personal Communications*, Vol. 7, No. 5, pp. 16-37, October 2000.

[32] Honghai Zhang and Jennifer C. Hou, “Maintaining Sensing Coverage and Connectivity in Large Sensor Networks,” *Wireless Ad Hoc and Sensor Networks: An International Journal*, Vol. 1, Num. 1-2, pp. 89-123, January 2005.

[33] Bhaskar Krisnamachari, Deborah Estrin, Stephen Wicker “Modeling Data-Centric Routing In Wireless Sensor Networks,” *USC Computer Engineering Technical Report CENG 02-14*, Los Angeles, California, April 2002.

[34] K. M. Sivalingam, “Tutorial on Wireless Sensor Network Protocols,” *International Conference on High-Performance Computing 2002*, Bangalore, India, December 2002.

[35] A. Nasipuri and K. Li, “A Directionality-Based Localization Scheme for Wireless Sensor Networks,” *Proceedings of Association for Computing Machinery Workshop on Wireless Sensor Networks and Applications 2002*, pp. 105-111, September 2002.

[36] Y. Ofek, "Generating a Fault-Tolerant Global Clock Using High-Speed Control Signals for the MetaNet Architecture," *IEEE/ACM Transactions on Networking*, Vol. 3, pp. 1650-1654, 2002.

[37] J. Elson and D. Estrin, "Time Synchronization for Wireless Sensor Networks," *Proceedings of IEEE IPDPS Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing 2001*, pp. 1965-1970. April 2001.

[38] C. Shen, C. Srisathapronphat, C. Jaikaeo, "Sensor Information Networking Architecture and Applications," *IEEE Personal Communications*, Vol. 8, No. 4, pp. 52 – 59, August 2001.

[39] N. Sastry and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks," *Web Information Systems Engineering* 2001, October 2004.

[40] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proceedings of IEEE Workshop on Sensor Networks Protocols and Applications 2003*, pp. 113-127, May 2003.

[41] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proceedings of Association for Computing Machinery Conference on Computer and Communications Security 2003*, pp. 62-72, October 2003.

[42] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion Tolerant Routing in Wireless Sensor Networks," *Technical Report CU-CS-939-02*, Department of Computer Science, University of Colorado, 2002.

[43] "MTS/MDA Sensor Board Users Manual," Rev. B, June 2006, Document 7430-0020-04. Crossbow Technology, Inc., San Jose, California. http://www.xbow.com/Support/wUserManuals.aspx, last accessed February 2007.

[44] J. Cham, B. Gee, G. Solis, and M. Linder, "Motes for Dummies," http://ece-classweb.ucsd.edu:16080/winter05/ece191/spring03/prj5/Final_prj5.ppt, last accessed March 2007.

[45] J. Suh and M. Horton, "Current Hardware and Software Technology for Sensor Networks," http://www-micrel.deis.unibo.it/~wsn/videowsn/pdf/H7.pdf, last accessed March 2007.

[46] "CC1000 Technical Information," Rev. 1.3, Chipcon AS, http://www.chipcon.com/files/CC1000_Data_Sheet_2_2.pdf, December 2004, last accessed February 2007.

[47] “ATmega128,” 2467M-AVR-11/04, http://www.atmel.com/dyn/resources/prod_documents/2467S.pdf, last accessed February 2007.

[48] “MoteWorks Getting Started Guide,” Rev. E, April 2007, Document 7430-0102-01. Crossbow Technology, Inc., San Jose, California. http://www.xbow.com/Support/wUserManuals.aspx, last accessed April 2007.

[49] “MPR/MIB Users Manual,” Rev. B, June 2006, Document 7430-0021-07. Crossbow Technology, Inc., San Jose, California. http://www.xbow.com/Support/wUserManuals.aspx, last accessed February 2007.

[50]J. L. Hill, *System Architecture for Wireless Sensor Networks*, Doctoral Dissertation, University of California, Berkeley, Berkeley, California, 2003.

[51] Tinyos Online Tutorial, http://www.tinyos.net/tinyos-1.x/doc/tutorial/, last accessed March 2007.

[52] “XMesh Users Manual,” Rev. D, April 2007, Document 7430-0108-01. Crossbow Technology, Inc., San Jose, California. http://www.xbow.com/Support/wUserManuals.aspx, last accessed April 2007.

[53] Crossbow Technologies, *Getting Started Guide and Reference Manuals*, Smart Dust Training Seminar, San Jose, 19-20 April 2005.

[54] Tim Reilly, “Mote Software Development for Wireless Sensor Networks,” presented at the Second Annual IEEE Communications Society Conference on Sensor and Ad-hoc Communications and Networks, Santa Clara, California, 26 September 2005.

[55] “Mote View Users Manual,” Rev. C, November 2006, Document 7430-0008-04. Crossbow Technology, Inc., San Jose, California. http://www.xbow.com/Support/wUserManuals.aspx, last accessed February 2007.

[56] Air Force Weather Agency Doctrine, CDC 1W051A (A Course), Vol.3, Tactical and Radio-Communications Equipment, Unit 3, Radio-Frequency Communication, http://www.fas.org/spp/military/docops/afwa/U3.htm, last accessed May 2007.

[57] Rodney Vaughan, http://www.science.ca/askascientist/viewquestion.php?qID=1767, last accessed April 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

2. Chair, Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

3. Professor John McEachen
   Naval Postgraduate School
   Monterey, California

4. Professor Weilian Su
   Naval Postgraduate School
   Monterey, California